

November 24, 2014

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

RE: ***Ex Parte Notice***; *Open Internet Remand Proceeding*, GN Docket No. 14-28; *Framework for Broadband Internet Service*, GN Docket No. 10-127; *Technology Transitions*, GN Docket No. 13-5; *A National Broadband Plan for Our Future*, GN Docket No. 09-51; *State of Wireless Competition*, WT Docket No. 13-135; *Broadband Industry Practices*, WC Docket No. 07-52

Dear Ms. Dortch:

Data Foundry, Inc. and Golden Frog, GmbH (“the companies”) give notice that they conducted a telephonic meeting with Gigi B. Sohn, Special Counsel for External Affairs, Office of the Chairman on November 20, 2014. Co-CEO Ron Yokubaitis, External Affairs Director Andrew MacFarlane and undersigned counsel participated for the companies.

The companies provided the attached documents to provide background and for reference. Specifically, the companies provided:

- Golden Frog initial comments (July 15, 2015)
- Verizon ex parte responding to Golden Frog (October 28, 2014)
- Golden Frog reply to Verizon ex parte (November 8, 2014)
- White paper: Beyond the Fourth Amendment: Additional Constitutional Implications
Arising From Big Government’s Surveillance and Seizures of U.S.
Citizens’ Digital Property
- Initial comments of the i2C (July 15, 2014)

The purpose of the telephonic meeting was to advise the Chairman’s office of the companies’ current views on the substance and merits of various proposals contained in the recent flurry of announcements and filings in the above-referenced proceedings. The conversation focused on problems with the so-called “hybrid” approach, Internet users’ freedom to choose services and applications unfettered by Internet access provider interference, and access provider invasions of users’ privacy.

The companies explained their opposition to so-called “hybrid” approach. The “hybrid” would not apply Title II to the most logical portion and the one that needs the greatest attention and authority: the last-mile transmission links between end users and the broadband Internet access provider. This is the portion where there is little to no competition or real customer choice. This is the “bottleneck.” The i2C comments comprehensively explained why Title II treatment for this portion is practically necessary and legally sustainable. The “hybrid” instead focuses on the so-called “back-end” even though the task at hand is making sure that end users have a full range of choices over what they do with the Internet access they purchase, and the place to do that is on the last mile. The rest will take care of itself.

Any concerns over the perceived “back-end” problem can easily be resolved through regulations addressing the access provider/end user relationship. The “back-end” problem arises only because the access providers are not doing what they need to do to fulfill the contractual commitments they made with their end users, namely providing a given level (capacity/speed) of access to the entire Internet. When access providers do not adequately upgrade capacity on the “back-end” their users do not get the broadband Internet access they were promised.

If the Commission decides to regulate some notional access provider/edge provider relationship then it will necessarily regulate edge providers, whatever the ultimate meaning of that term.¹ WTA² and NCTA³ have already asked the Commission to bring the entire Internet “ecosystem” within Title II. More recently, NCTA asked the Commission to impose regulations on “edge providers” using 706.⁴ It is therefore plain that regulating the access provider/edge provider “relationship” will surely and quickly turn into substantive and direct regulation over edge providers. The Commission could condition a continued “relationship” on meeting virtually any condition that comes to mind. NTCA, for example, wants the Commission to impose a “no blocking” rule to preclude ... so-called ‘content’ or ‘edge’ providers from denying basic consumer access to content, applications, or services that are otherwise available on the Internet.”⁵ The Commission recently reaffirmed a decision to impose a somewhat similar “no blocking” rule on non-carrier “intermediate providers”⁶ using Title I “ancillary authority.”⁷ But the regulation could just as easily include a requirement to block certain content, services, or

¹ The term “edge provider” was first defined in *Preserving the Open Internet*, Report and Order, 25 FCC Rcd 17905, 17907, ¶4, n. 2 (2010) (“*Open Internet Order*”), aff’d in part, vacated and remanded in part *sub nom. Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014). (“We use “edge provider” to refer to content, application, service, and device providers, because they generally operate at the edge rather than the core of the network.”). The Commission proposed a slightly different definition in *See Open Internet Remand NPRM*, proposed rule 8.11(c) (“(c) Edge Provider. Any individual or entity that provides any content, application, or service over the Internet, and any individual or entity that provides a device used for accessing any content, application, or service over the Internet.”) Both definitions are extraordinarily broad, with the result that “edge provider” ultimately means any entity or person other than an access provider that does anything besides passively download information.

² WTA July 17, 2014 comments, pp. 3-4.

³ NTCA Comments, July 18th, 2014. These comments are wholly dedicated to a request that the Commission apply Title II and 706 to impose regulations over the entire Internet “ecosystem.”

⁴ NTCA’s *ex parte* from November 13 again seeks regulation over edge providers, supposedly under the “hybrid” theory.

⁵ NTCA July 18, 2013 Comments, pp. 2, 14-17.

⁶ “Intermediate provider” is defined in rule 64.1600(f) (“Intermediate Provider. The term Intermediate Provider means any entity that carries or processes traffic that traverses or will traverse the PSTN at any point insofar as that entity neither originates nor terminates that traffic.”) The concept is quite similar to the meaning and effect of “edge provider.” Indeed, some of the scholarly treatment refers to “intermediaries” rather than “edge providers.” See, e.g., Christiaan Hogendorn, *Broadband Internet: Net Neutrality versus Open Access*, p. 4, International Economics and Economic Policy 4, 185-208 (2007), available at <http://chogendorn.web.wesleyan.edu/oa.pdf>. (“Like telephone resellers, intermediaries are the middlemen between the conduit and the content, but unlike in telephone, they are not common carriers with regard to content.”)

⁷ Order on Reconsideration, *In the Matter of Rural Call Completion*, WC Docket No. 13-39, FCC 14-175, ¶¶51-56, 2014 FCC LEXIS 4273 *71-*79 (November 13, 2014).

applications or even content. Once again, there is precedent: in 2012 the Commission asked if it should “require CMRS providers to take steps to prevent the use of certain third-party applications that do not support text-to-911.” In other words, the Commission was thinking about requiring wireless broadband Internet access providers to block Internet applications that did not meet certain Commission-preferred criteria.⁸

The problem at hand has nothing to do with “edge provider” activity and the Commission should not undertake to regulate edge providers, whose conduct is not properly a matter of Commission concern. The problem is the lack of competition in the last mile, and the resulting ability of the dominant providers to interfere with their own users’ efforts to actually use and enjoy the full Internet, with all of its capabilities. Despite what all the “abuse deniers” claim, there has been abuse in the past, and it continues to this day. i2C, Golden Frog and many others have provided an extraordinary amount of information and examples demonstrating that the dominant last mile providers have the incentive and ability to take, and have taken, undue advantage of the gate-keeping power they have over consumer choices regarding how they use the Internet, the Internet-related applications, services and devices they enjoy, and the content they generate and want to receive.

This takes us to the second topic discussed during the call. Golden Frog’s initial comments and the November 8, 2014 reply to Verizon’s *ex parte* response addressed abuses on the “user-facing” side. For example, Golden Frog explained that access providers currently inspect unencrypted traffic that comes from or goes to their users, within their networks and not necessarily at the edge of the network. They monitor the content of their users’ Internet communications when they can. They use this knowledge of the content for their own advantage and disclose it to others, including the government. They perform application identification and unilaterally apply “special treatment” to some applications – either slowing or assigning priority using as-yet unknown criteria – on unencrypted traffic. Golden Frog proved that at least one wireless broadband Internet access provider was blocking its users’ efforts to maintain the privacy and security of their own traffic through encryption. Golden Frog explained that neither the now-vacated former rules nor the NPRM proposed rules in any way prevented or would prevent access provider encryption blocking, for either wireless or wireline broadband Internet access.

The companies urged Chairman Wheeler to not get distracted from the true problem at hand and to apply appropriate regulations to address that problem. The problem is the last mile. The lack of competition is negatively impacting the dominant access provider/end user “relationship.” If the Commission does not return to the original open access framework that gave us the Internet, then it must stay focused on the provider/end user “relationship.” It can completely solve any perceived issues with the “back-end” by simply requiring access providers to actually do what they contractually promised to do: deliver their end user the contracted level (capacity/speed) of access to the entire Internet, not just the part the access provider likes or the

⁸ Further Notice of Proposed Rulemaking, *In the Matter of Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications; Framework for Next Generation 911 Deployment*, 27 FCC Rcd 15659, 15723, ¶171 (2012).

Ms. Marlene H. Dortch, Secretary - Federal Communications Commission

RE: **Ex Parte Notice**; *Open Internet Remand Proceeding*, GN Docket No. 14-28; *Framework for Broadband Internet Service*, GN Docket No. 10-127; *Technology Transitions*, GN Docket No. 13-5; *A National Broadband Plan for Our Future*, GN Docket No. 09-51; *State of Wireless Competition*, WT Docket No. 13-135; *Broadband Industry Practices*, WC Docket No. 07-52

part from which the access provider can extort access tolls. Access providers must also be prevented from unilaterally inspecting and appropriating user content – which is their *property*⁹ – or blocking users’ efforts to encrypt their traffic in order to maintain control over their privacy, security and property.

Sincerely,

/s/

W. Scott McCollough
Counsel to Data Foundry, Inc. and
Golden Frog GmbH

Attachments

xc: Gigi Sohn, via email
Jonathan Sallet, General Counsel, via email
Stephanie Weiner, Associate General Counsel, via email

⁹ See attached White paper: Beyond the Fourth Amendment: Additional Constitutional Implications Arising From Big Government’s Surveillance and Seizures of U.S. Citizens’ Digital Property.

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)	
)	GN Docket No. 14-28
Protecting and Promoting the Open Internet)	

In the Matter of)	
)	GN Docket No 10-127
Framework for Broadband Internet Service)	

In the Matter of)	
)	GN Docket No. 13-5
Technology Transitions)	

In the Matter of)	
)	GN Docket No. 09-51
A National Broadband Plan for Our Future)	

In the Matter of)	
)	WT Docket No. 13-135
State of Wireless Competition)	

In the Matter of)	
)	WC Docket No. 07-52
Broadband Industry Practices)	

COMMENTS OF GOLDEN FROG

Matthew A. Henry
henry@dotlaw.biz
W. Scott McCollough
wsmc@dotlaw.biz
MCCOLLOUGH|HENRY PC
1250 S. Capital of Texas Hwy., Bldg. 2-235
West Lake Hills, TX 78746
Phone: 512.888.1112
Fax: 512.692.2522

July 18, 2014

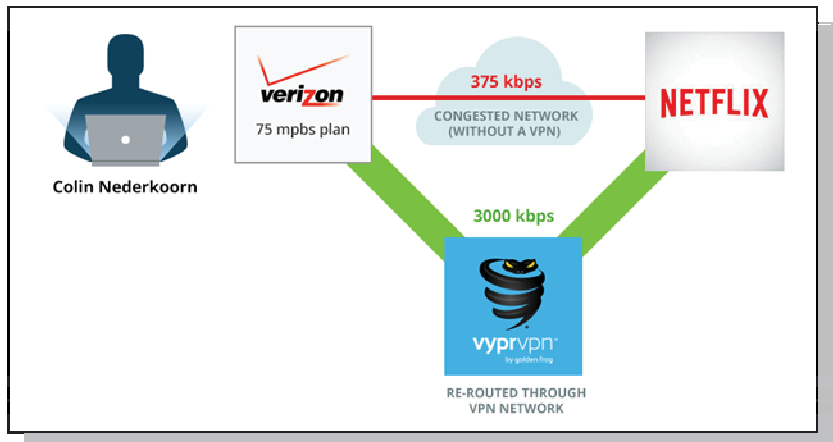
TABLE OF CONTENTS

I.	EXECUTIVE SUMMARY	1
II.	DESCRIPTION OF GOLDEN FROG	2
II.	VPNs PROTECT PRIVACY AND SHOW THAT INTERNET ACCESS PROVIDERS ARE THROTTLING TRAFFIC	4
III.	ENCRYPTION BLOCKING IS OCCURRING TODAY AND THE PROPOSED RULES WOULD NOT STOP IT	7
IV.	CONCLUSION.....	10
ATTACHMENT A: NETFLIX THROUGH CONGESTED NETWORK COMPARED TO THROUGH A VPN		
ATTACHMENT B: OVERWRITING STARTTLS ENCRYPTION SESSION INITIATION		

I. EXECUTIVE SUMMARY

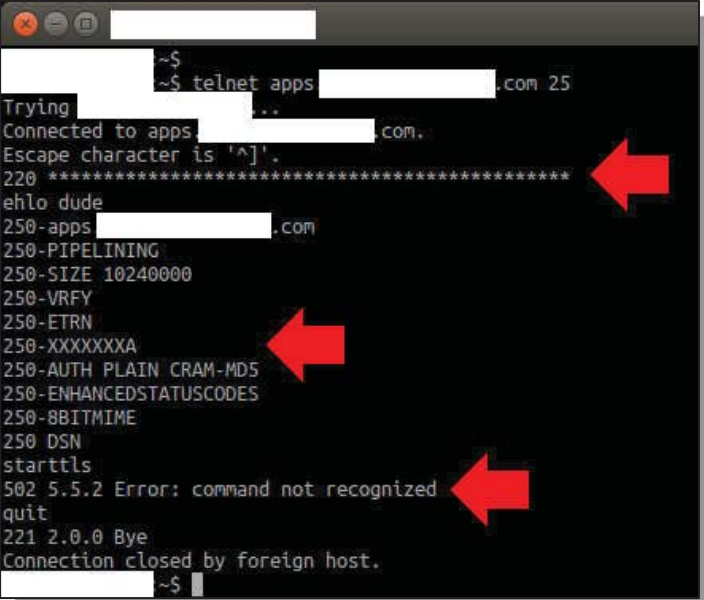
Since there are no enforceable open Internet rules, broadband Internet access providers are currently throttling and blocking Internet users' traffic. These comments discuss two recent examples that show that users are not receiving the open, neutral, and uninterrupted service to which the Commission says they are entitled.

In the first instance, a customer of Golden Frog's VyprVPN encrypted VPN service has proven that his Netflix traffic is being throttled on Verizon's FiOS service. Colin Nederkoorn recently



posted a YouTube video of a test he performed on his 75 Mbps service from Verizon that shows his Netflix connection increased from a paltry 375 Kbps to 3000 Kbps when he employed VyprVPN. This is a ten-fold increase that resulted from encrypting his traffic and using VyprVPN's routing. This type of increase in speed is consistent with reports from other customers. Internet access providers are "mismanaging" their networks to their own users' detriment.

In the second instance, Golden Frog shows that a wireless broadband Internet access provider is interfering with its users' ability to encrypt their SMTP email traffic. This broadband provider is overwriting the content of users' communications and actively blocking STARTTLS encryption. This is a man-in-the-middle attack that



The screenshot shows a terminal window with a telnet session to 'apps[REDACTED].com'. The user enters 'telnet apps[REDACTED].com 25'. The session shows SMTP protocol messages: '220 *****', 'ehlo dude', '250-apps[REDACTED].com', '250-PIPELINING', '250-SIZE 10240000', '250-VRFY', '250-ETRN', '250-XXXXXXA', '250-AUTH PLAIN CRAM-MD5', '250-ENHANCEDSTATUSCODES', '250-8BITMIME', '250 DSN', 'starttls', and '502 5.5.2 Error: command not recognized'. The session ends with 'quit', '221 2.0.0 Bye', and 'Connection closed by foreign host.' Three red arrows point to the lines '220 *****', '250-XXXXXXA', and '502 5.5.2 Error: command not recognized'.

```
~$  
~$ telnet apps[REDACTED].com 25  
Trying [REDACTED]...  
Connected to apps[REDACTED].com.  
Escape character is '^['.  
220 *****  
ehlo dude  
250-apps[REDACTED].com  
250-PIPELINING  
250-SIZE 10240000  
250-VRFY  
250-ETRN  
250-XXXXXXA  
250-AUTH PLAIN CRAM-MD5  
250-ENHANCEDSTATUSCODES  
250-8BITMIME  
250 DSN  
starttls  
502 5.5.2 Error: command not recognized  
quit  
221 2.0.0 Bye  
Connection closed by foreign host.  
~$
```

prevents customers from using the applications of their choosing and directly prevents users from protecting their privacy.

The Commission must establish effective rules that prevent this type of behavior. Unless wireless and wireline broadband access providers receive a strong message that they can no longer throttle and block their users' Internet traffic, these actions will continue, expand, and become the norm. Golden Frog calls on the Commission to truly restore the open Internet, enhance competition, protect user choice, and ensure users can keep nosy Internet access providers from intercepting their private information.

II. DESCRIPTION OF GOLDEN FROG

Golden Frog GmbH¹ is a global service provider committed to developing applications and services that provide an open and secure Internet experience, while preserving and enhancing user privacy. Golden Frog owns and operates a global network with private server

¹ Golden Frog is a member of the Internet Infrastructure Coalition (i2Coalition), and supports the comments submitted by the i2Coalition. Like i2Coalition, Golden Frog believes that a preferable course of action is to return to Open Access, and if this is done the Commission need not and should not directly regulate Internet access.

clusters in North America, South America, Europe, Asia and Oceania with users in over 195 countries. Golden Frog owns and manages 100% of its own servers, hardware and network to ensure the highest levels of security, privacy and service delivery. Golden Frog's founders are Internet veterans who have owned and operated Internet businesses since the dawn of the public Internet in 1994.

Golden Frog created VyprVPN – a secure personal VPN service – to help users protect themselves against efforts by commercial or governmental third parties to monitor, access and intercept confidential, privileged or private information. VyprVPN provides encrypted connections to the Internet to protect user privacy and security. Like other VPN providers, Golden Frog uses standards-based VPN protocols. Unlike other VPN providers, Golden Frog writes 100% of its supporting software, manages its own network, and owns the hardware enabling it to deliver the fastest VPN speeds in the world. VyprVPN has desktop applications for Windows and Mac and recently launched mobile apps for iOS and Android.

Dump Truck is Golden Frog's second product. Dump Truck provides secure online storage that allows users to safely store, sync, share and access all of their files from anywhere and on any device. All data uploaded to Dump Truck is encrypted in transit and then encrypted with per-user keys while stored. Golden Frog does not rely on third parties to store user data or use data deduplication to inspect user data. Dump Truck for Mac and Windows automatically syncs all files to the desktop. Dump Truck mobile apps for iOS and Android allow easy access to files while on the go. The Dump Truck Web App provides access to files from any web browser and access to advanced features such as public sharing, activity feeds, and more.

II. VPNs PROTECT PRIVACY AND SHOW THAT INTERNET ACCESS PROVIDERS ARE THROTTLING TRAFFIC

Golden Frog's original purpose for VyprVPN was to protect privacy and facilitate a truly open Internet. Even before the Snowden revelations, we were aware of the extent to which both government and other commercial interests were inspecting traffic and monitoring domestic communications. Indeed, our sister company Data Foundry predicted this would occur in multiple prior filings with the Commission.² When the Commission and others chose to proceed despite Data Foundry's cautioning, our founders decided to deploy a product that would defeat monitoring efforts. At the same time, several other countries were also spying on their citizens and denying access to Internet applications, content, services, uses, sources/destinations or devices. Golden Frog was formed, and VyprVPN was born. Users worldwide can now access the full Internet and maintain privacy using our encryption tools.

² Docket 07-52, *In the Matter of Broadband Industry Practices*, Data Foundry Comments, pp. 9-12 and Attachment B (June 16, 2007), available at <http://apps.fcc.gov/ecfs/document/view?id=6519529007>; Docket 07-52, *In the Matter of Broadband Industry Practices*, Data Foundry Reply Comments (July 16, 2007), available at <http://apps.fcc.gov/ecfs/document/view?id=6519558239>; Docket 07-52, *In the Matter of Broadband Industry Practices*, Data Foundry Notice of *Ex Parte* and Attachment "Tiered Internet Service Threatens the Privileged and Confidential Nature of Online Communications" (October 22, 2008), available at <http://apps.fcc.gov/ecfs/document/view?id=6519741393>; Docket 07-52, *In the Matter of Broadband Industry Practices*, Data Foundry Notice of *Ex Parte* and Attachment "Broadband Network Management and Net Neutrality: Equal Threats to User Privacy and Security" (October 22, 2008), available at <http://apps.fcc.gov/ecfs/document/view?id=6520176853>; Docket GN 09-51, *In the Matter of A National Broadband Plan for Our Future*, Data Foundry Comments (June 8, 2009), available at <http://apps.fcc.gov/ecfs/document/view?id=6520220238>; Docket GN 09-51, *In the Matter of A National Broadband Plan for Our Future*, Data Foundry Reply Comments (July 21, 2009), available at <http://apps.fcc.gov/ecfs/document/view?id=7019917828>; Docket 07-52, *In the Matter of Broadband Industry Practices* and Docket GN 09-51, *In the Matter of A National Broadband Plan for Our Future*, Data Foundry Notice of *Ex Parte* (October 19, 2009), available at <http://apps.fcc.gov/ecfs/document/view?id=7020142373>; GN Docket 09-191, *In the Matter of Preserving the Open Internet* and WC Docket 07-52, *Broadband Industry Practices*, Data Foundry Comments (January 14, 2010), available at <http://apps.fcc.gov/ecfs/document/view?id=7020378808>; NBP Public Notice #29, GN Docket Nos. 09-47, 09-51, and 09-137, Data Foundry Comments (January 23, 2010), available at <http://apps.fcc.gov/ecfs/document/view?id=7020383064>; GN Dockets No. 09-51 and 09-191 and WC Docket No. 07-52, Data Foundry Notice of *Ex Parte* and Attachment (January 28, 2010), available at <http://apps.fcc.gov/ecfs/document/view?id=7020384236>; GN Docket No. 10-127, *In the Matter of Framework for Broadband Internet Service*, Data Foundry Comments, pp. 23-35 (July 15, 2010), available at <http://apps.fcc.gov/ecfs/document/view?id=7020547123>; GN Docket No. 10-127, *In the Matter of Framework for Broadband Internet Service*, Data Foundry Reply Comments, pp. 16-22 (August 12, 2010), available at <http://apps.fcc.gov/ecfs/document/view?id=7020706608>; ; GN Docket No. 10-127, *In the Matter of Framework for Broadband Internet Service*, Data Foundry Notice of *Ex Parte* (August 25, 2010), available at <http://apps.fcc.gov/ecfs/document/view?id=7020809986>.

VPNs, however, have another salutary attribute. They defeat Internet access provider throttling through application identification and “special treatment” on the user facing side or purposeful congestion of particular connections on the “Internet” facing side. VyprVPN, in effect, allows Internet access customers to override Internet access providers’ privacy invasions and other conduct that inhibits, interferes with or controls user choices regarding applications, content, services, use, source/destination or devices.

VyprVPN users consistently report that their speeds increase when they use VyprVPN. They are effectively using VyprVPN’s encrypted connection to boost their speeds, while also protecting their privacy. This demonstrates that there is a market for alternative Internet access providers that do not throttle traffic or invade their users’ privacy, and VPNs are proving to be the closest surrogate for real broadband competition

The current controversy over whether Internet service providers are throttling video traffic or purposefully letting traffic become congested on ingress links demonstrates this is so. Several users that suffer degraded video streams when trying to connect to video sites like Netflix or YouTube have discovered that if they employ a VPN, the problem disappears. A recent example was revealed on July 17, 2014.³ Golden Frog has known about this for quite some time. For example, we blogged about the issue in April, 2014.⁴

Common sense would lead one to believe speeds would inherently slow down due to the encryption overhead. But activity at the network layer explains why there is increased speed

³ See Colin Nederkoorn’s Blog, *Verizon made an enemy tonight*, <http://iamnotaprogrammer.com/Verizon-Fios-Netflix-Vyprvpn.html>; John Brodtkin, ‘Verizon made an enemy’: FiOS customer mad that Netflix works better on VPN, 75Mbps Verizon FiOS service isn’t good enough to stream Netflix smoothly, *Ars Technica* (July 18, 2014), available at <http://arstechnica.com/information-technology/2014/07/verizon-made-an-enemy-fios-customer-mad-that-netflix-works-better-on-vpn>; Ben Popper, *How one man bypassed internet congestion and fixed his Netflix streaming*, *On today’s internet, the shortest route is sadly not always the best*, *The Verge* (July 18, 2014), available at <http://www.theverge.com/2014/7/18/5916153/netflix-verizon-vpn-streaming-congestion-speed>.

⁴ See Golden Frog Blog, *Infographic: Netflix vs. Comcast – The Peering Problem*, (April 25, 2014) © 2014 Golden Frog, GmbH, available at <http://www.goldenfrog.com/blog/netflix-vs-comcast-the-peering-problem>.

despite the additional overhead. A VPN provider that operates its own server infrastructure, is multi-homed, and that runs its own network can control the router and dynamically use uncongested routes to users.⁵ Attachment A provides an illustration. The Internet access providers are using Deep Packet Inspection to identify the application, content, service, use, source/destination or device based on access provider preferences, rather than user preferences. Proxies and encryption allow the user to override the Internet access provider's "traffic management" and shaping.

Of particular interest in the example from July 17 is that this consumer was able to utilize the same Internet access to achieve full throughput of his Netflix service by using a VPN to control the route through which Netflix flowed. This demonstrates that his Internet access provider has sufficient bandwidth to fulfill his request, but the provider chooses to not properly manage the network in order to provide their customer the bandwidth that was advertised and contracted. Instead, he had to take further action and utilize a VPN service, in the hopes that the route through his Internet access provider to the VPN service was on an uncongested link.

The Internet access providers may claim that alternatives such as VyprVPN provide the sort of technological or competitive market responses available on the Internet that make rules unnecessary. While it is true that these are in fact technological and competitive market responses, the very same Internet access providers who make that claim can throttle or block VPNs, proxies or encryption if the Commission imposes no effective rules. As the i2Coalition observed in its comments on pages 37-49, the current proposed rules do not prevent them from

⁵ The large Internet access providers could use similar network management techniques avoid congestion on ingress and egress traffic, but they choose to not do so. If they had any competition or a true desire to actually fulfill the contracts they formed with their users they would add capacity as needed and use real management rather than opportunistically attacking traffic they do not like or want to tax.

interfering with encryption services. Without enforceable rules, Netflix throttling may be the problem of today and encryption blocking the problem of tomorrow.

We turn now to a demonstration that broadband Internet access providers have already started blocking their users' efforts to encrypt.

III. ENCRYPTION BLOCKING IS OCCURRING TODAY AND THE PROPOSED RULES WOULD NOT STOP IT

As a result of *Verizon v. FCC*, broadband Internet access providers are no longer subject to any no-blocking or anti-discrimination rules.⁶ They are completely free to interfere with their customers' use of the Internet at will. The dominant Internet access providers repeatedly protest that rules against blocking and unreasonable discrimination need not be reinstated because there is no evidence any is occurring or will occur, and they can be trusted to act properly without any rules. The NPRM, however, sets out actual empirical evidence supporting the stated concerns by listing a series of acts by fixed and mobile Internet access provider that directly support those concerns.⁷ Our Netflix example above provides further evidence of an Internet access provider failing to perform proper network management in the best interest of fulfilling the service sold to a large number of customers.

The purpose of these comments is to provide new evidence that blocking is occurring today, and therefore demonstrate that there are still problems to be solved and effective rules are required. Golden Frog has recently discovered that at least one broadband service provider is blocking the use of a common email encryption technology. Specifically, this provider is using network equipment to block the STARTTLS command from enabling the encryption of SMTP (Simple Mail Transfer Protocol) traffic.

⁶ *Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014).

⁷ *Protecting and Promoting the Open Internet*, Notice of Proposed Rulemaking, 2014 FCC LEXIS 1689 (2014) at ¶¶ 6, 26, and 39-53.

STARTTLS is an extension to SMTP that allows an SMTP server and client to use TLS (Transport Layer Security) to provide private, encrypted, and authenticated communication over the Internet. This gives users the ability to protect some or all of their communications from eavesdroppers and attackers. SMTP [RFC2821] servers and clients routinely communicate in the clear over the Internet.⁸ In many cases, this communication goes through one or more routers that are not controlled or trusted by either entity. An untrusted router might allow a third party to monitor or alter the communications between the server and client.⁹

STARTTLS allows a client to initially make a clear connection but then initiate a request to the server to switch to an encrypted connection. The initial connection is in the clear, so any entity in the middle – including the Internet access provider – can see the connection requests and associated header and control information, including the connection set up requests. It is possible for an Internet access provider to interpret the request and control information, and to even change the content requests from the client or responses from the server. This includes the client request to initiate an encrypted session, or the server response to that request.

Golden Frog performed tests using one mobile wireless company's data service, by manually typing the SMTP commands and requests, and monitoring the responses from the email server in issue. It appears that this particular mobile wireless provider is intercepting the server's banner message and modifying it in-transit from something like "220 [servername] ESMTP Postfix" to "200 *****." The mobile wireless provider is further modifying the server's response to a client command that lists the extended features supported by the server. The mobile wireless provider modifies the server's "250-STARTTLS" response

⁸ It is possible to establish an encrypted connection at the beginning. SMTPS automatically starts SSL encryption before any SMTP level communication.

⁹ RFC 3207, SMTP Service Extension for Secure SMTP over Transport Layer Security, © The Internet Society (2002), available at <https://tools.ietf.org/html/rfc3207>.

(which informs the client of the server's capacity to enable encryption). The Internet access provider changes it to "250-XXXXXXA." Since the client does not receive the proper acknowledgement that STARTTLS is supported by the server, it does not attempt to turn on encryption. If the client nonetheless attempts to use the STARTTLS command, the mobile wireless provider intercepts the client's commands to the server and changes it too. When it detects the STARTTLS command being sent from the client to the server, the mobile wireless provider modifies the command to "XXXXXXX." The server does not understand this command and therefore sends an error message to the client.

The practice in issue and in use by this provider is conceptually similar to the way that Comcast used packet reset headers to block the use of BitTorrent in 2007. The result is that wireless Internet users that wish to protect their email communications with basic encryption protocols cannot do so when on this particular wireless provider's network.

Although the precise technology being used in this instance cannot be determined, the activity resembles a documented feature made available in the Cisco Adaptive Security Appliance (ASA). An ASA purchaser can engage in "ESMTP application inspection," monitor content, and limit commands and responses that that can pass through the system. Cisco's documentation explains that after the ASA purchaser enables ESMTP application inspection, the feature "changes the characters in the server SMTP banner to asterisks." "An SMTP server responds to client requests with numeric reply codes and optional human readable strings. SMTP application inspection controls and reduces the commands that the user can use as well as the messages that the server returns."¹⁰ This is exactly what Golden Frog experienced.

¹⁰ The Cisco Adaptive Security Appliance's ability to filter SMTP and ESMTP traffic is documented and explained at <http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113423-asa-esmtp-smtp-inspection.html>; see also <http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/I-R/cmdref2/i2.html#pgfId-1765148>. Golden Frog is not alleging that the blocking related above is being performed

Attachment B to these comments contains two screenshots that compare a successful STARTTLS session initiation (on a different network) with a failed session on the wireless provider's network. The screenshot of the unsuccessful STARTTLS session shows that an ESMTP banner is being overwritten with asterisks, the STARTTLS extended option is Xed out, and the client command leads to an error message. The result is an inability to establish an encrypted link.

Absent enforceable Commission rules, broadband providers can (and at least one already does) block and discriminate against entirely acceptable Internet uses. In this case, users are not just losing their right to use the applications and services of their choosing, but also their privacy. It is not at clear that this type of encryption blocking would be forbidden for fixed broadband Internet access, under the proposed rules' exception for reasonable network management. This example involves mobile wireless broadband, however, and it is clear that the proposed rules would not prohibit the activity. STARTTLS encryption does not constitute "a lawful website" or "an application[] that compete[s] with the provider's voice or video telephony services[.]"¹¹ The proposed rules on their face do not prohibit mobile broadband Internet access providers from blocking user efforts to maintain privacy through encryption.

IV. CONCLUSION

The claim that rules banning blocking and unreasonable discrimination are solutions in search of a problem is flatly wrong. There have been problems in the past and there are problems

by a Cisco appliance. The citation and quotations are provided only to provide a technical explanation of how it can be made to occur, and the result. Further, Golden Frog emphasizes that this feature can be important to an Enterprise or private network operator to manage security issues. The problem arises when it is applied by an Internet access provider to conduct a man in the middle attack in order to frustrate a user's efforts to encrypt communications and perhaps even intercept the content of emails the user wants to keep private. In this situation, the Internet access provider is merely "an untrusted router" and "third party" that is able to monitor or alter the communications between the server and client." As RFC 3207 explains that is the very thing the STARTTLS extension is designed to prevent.

¹¹ See *Protecting and Promoting the Open Internet*, Notice of Proposed Rulemaking, 2014 FCC LEXIS 1689 (2014) at § 8.5.

now. The proposed rules do not resolve all of the problems identified in the NPRM. Further broadband Internet access providers are still interfering with beneficial and privacy-enhancing applications users want to employ. Internet access providers, even with demonstrable available bandwidth, also continue to fail to properly manage the networks to ensure their customer base receives the service levels they have contracted for and paid to receive. The Commission needs to take strong action to protect the Open Internet. The proposed rules fall far short.

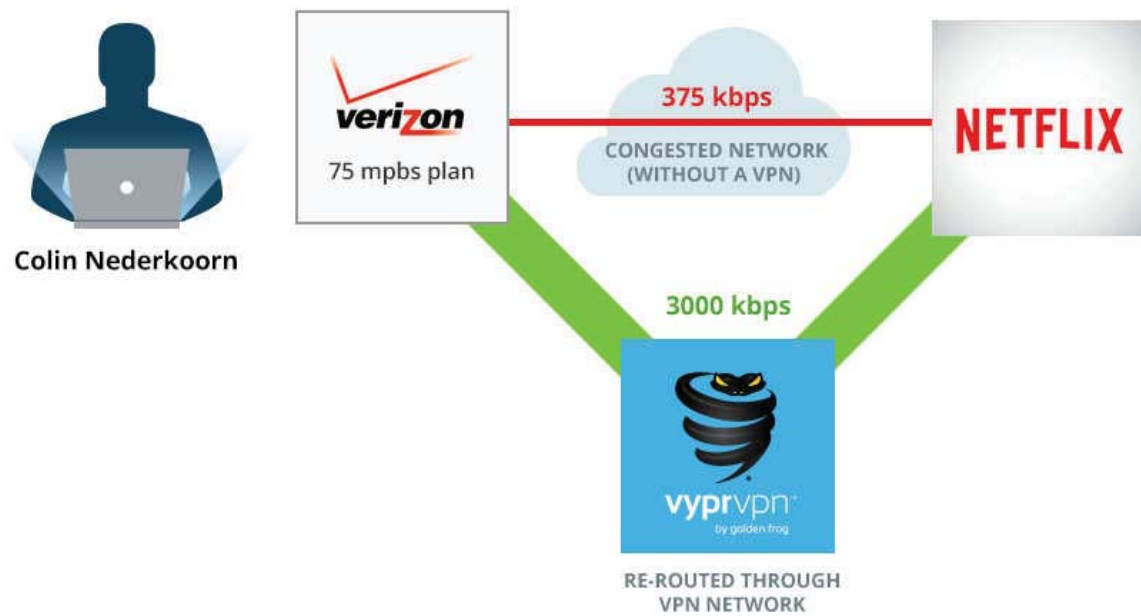
Respectfully Submitted,

Matthew A. Henry
henry@dotlaw.biz
W. Scott McCollough
wsmc@dotlaw.biz
MCCOLLOUGH|HENRY PC
1250 S. Capital of Texas Hwy., Bldg. 2-235
West Lake Hills, TX 78746
Phone: 512.888.1112
Fax: 512.692.2522

July 18, 2014

ATTACHMENT A

NETFLIX THROUGH CONGESTED NETWORK COMPARED TO THROUGH A VPN



ATTACHMENT B

OVERWRITING STARTTLS ENCRYPTION SESSION INITIATION

A. Normal STARTTLS Encryption Initiation Response

```
~$ telnet apps [redacted] com 25
Trying [redacted] ...
Connected to apps [redacted] com.
Escape character is '^]'.
220 apps [redacted] com ESMTP Postfix (Ubuntu)
ehlo dude
250-apps [redacted] com
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN CRAM-MD5
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
starttls
220 2.0.0 Ready to start TLS
^]close

telnet> close
Connection closed.
~$
```

B. Network-Overwritten STARTTLS Encryption Initiation Response

```
~$
~$ telnet apps [redacted] com 25
Trying [redacted] ...
Connected to apps [redacted] com.
Escape character is '^]'.
220 *****
ehlo dude
250-apps [redacted] com
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-XXXXXXA
250-AUTH PLAIN CRAM-MD5
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
starttls
502 5.5.2 Error: command not recognized
quit
221 2.0.0 Bye
Connection closed by foreign host.
~$
```

Roy E. Litland
Assistant General Counsel



1320 N. Courthouse Road
9th Floor
Arlington, VA 22201
Phone 703-351-3160
Fax 703-351-3664
roy.litland@verizon.com

October 28, 2014

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Re: *Open Internet Remand Proceeding, GN Docket No. 14-28*
Framework for Broadband Internet Service, GN Docket No. 10-127
Technology Transitions, GN Docket No. 13-5
A National Broadband Plan for Our Future, GN Docket No. 09-51
State of Wireless Competition, WT Docket No. 13-135
Broadband Industry Practices, WC Docket No. 07-52

Dear Ms. Dortch:

In comments filed in the above-captioned proceedings, Golden Frog, a provider of virtual private network (VPN) services, alleged that “broadband Internet access providers are currently throttling and blocking Internet users’ traffic,” and specifically alleged that an unnamed mobile broadband provider “is interfering with its users’ ability to encrypt their SMTP email traffic” and that U.S. Internet access providers, including Verizon, are throttling Netflix Internet traffic.¹ At least with respect to Verizon, Golden Frog’s allegations are unfounded.

Golden Frog’s Encryption-Blocking Claim

In its comments, Golden Frog claims it has “new evidence” that an unspecified mobile wireless company is “blocking the use of a common email encryption technology.”² In particular, Golden Frog alleges that “this provider is using network equipment to block the STARTTLS command from enabling the encryption of SMTP (Simple Mail Transfer Protocol) traffic.”³ As evidence, Golden Frog provides two redacted computer screen shots of DOS

¹ See July 18, 2014 Golden Frog Comments at 1-2.

² Golden Frog Comments at 7-8.

³ Golden Frog Comments at 7.

commands and responses that it claims show that the unnamed mobile wireless company somehow overrode Golden Frog's attempt to initiate encryption.⁴

While, without more detail, it is difficult to know what may have caused the results Golden Frog claims it observed, we can confirm that Verizon does not have a policy or practice of blocking end users' chosen encryption. Period.

Moreover, based on the information included in the Golden Frog comments, our engineers have attempted to replicate the steps described by Golden Frog to ensure that no blocking was inadvertently taking place. The network team ran the same routines that Golden Frog apparently ran. Using those routines, we successfully enabled encryption on both our wireless and wireline networks. While our tests confirmed that the allegation is not true with respect to Verizon's network, in the view of our network engineers, Golden Frog's computer screenshots and accompanying explanation do not provide enough information to say why Golden Frog apparently could not enable encryption or to demonstrate that an ISP's policy or practice was responsible. For example, the information provided by Golden Frog's screen shots could just as easily be consistent with an issue with network conditions and settings controlled by Golden Frog or a remote network.

Golden Frog's Throttling Allegation

Golden Frog's comments also erroneously claim that Verizon throttled Netflix traffic over subscribers' last-mile connections—a baseless allegation that Verizon has previously rebutted. As evidence, Golden Frog relies on the blog of a FiOS customer claiming that in July of this year he experienced significantly faster Netflix streaming speeds when he used Golden Frog's VyperVPN than when he did not use the VPN.⁵ Golden Frog asserts that this proves that the customer's "Netflix traffic is being throttled on Verizon's FiOS service" and Golden Frog provides a diagram suggesting that Verizon has a "congested network."⁶ Golden Frog's claims are inaccurate and misleading.

As researchers at MIT led by David Clark recently noted, there is not a "widespread congestion problem among the U.S. providers."⁷ The MIT report also noted that congestion on the Internet often resulted from "decisions by content providers [such as Netflix] as to how to route content," which can result in sudden congestion problems.⁸ As explained in Verizon's opening comments, our investigation into the cause of slow Netflix streaming experienced by

⁴ Golden Frog Comments at 8-10, Attach. B.

⁵ Golden Frog Comments at 1, 5-6.

⁶ Golden Frog Comments at 1, Attach. A.

⁷ MIT Information Policy Project, *Measuring Internet congestion: A preliminary report*, at 2 (2014), <https://ipp.mit.edu/sites/default/files/documents/Congestion-handout-final.pdf> (last visited Oct. 27, 2014).

⁸ *Id.*

another FiOS customer earlier this year confirmed the MIT report's view.⁹ We found that the congested Netflix traffic was caused by Netflix's previous decision to route its traffic over a handful of transit providers who had not made arrangements for connections that could handle Netflix's traffic volumes, while the other peering and transit providers and content providers interconnecting with Verizon's network in the customer's area were not experiencing congestion.

In April, Verizon and Netflix entered a voluntary commercial arrangement to directly interconnect with each other. With this arrangement, Netflix directly hands off its traffic destined for subscribers on Verizon's broadband networks, thus establishing a stable and predictable way of handling the large volumes of traffic associated with Netflix service and improving the consumer experience. And now that the agreement has been substantially implemented, that is exactly what has happened. This agreement provides further evidence that the existing and long-standing process for handling Internet interconnection through voluntary, commercial negotiations works, providing incentives for all parties to reach efficient interconnection arrangements that serve end-user consumers well.

Here, the customer evidence cited by Golden Frog is consistent with Verizon's previous findings related to Netflix's reliance on congested peering ports to reach Verizon customers. In particular, when the customer went directly to the Netflix site, the traffic sent by Netflix likely was directed over peering ports that, at the time, were experiencing substantial levels of congestion. In contrast, when the same customer used a VPN to access Netflix, it is very likely that the VPN travelled over a different interconnection path that did not include those same congested peering ports. So, by way of illustration, when accessing Netflix via a VPN, the interconnection path may have looked something like this:

Netflix → Transit Provider 1 → VPN → Transit Provider 2 → Verizon → customer

If there is no congestion in these interconnection paths, including on the various transit providers' networks and at the points where each of the various networks interconnect, then the customer would experience high quality speeds for the Netflix traffic even though he was accessing the traffic via a VPN. In contrast, if the customer does not use the VPN and receives the Netflix traffic directly, the interconnection path may have looked more like this:

Netflix → Transit Provider 3 → Verizon → customer

If there is congestion on Transit Provider 3's network or if Transit Provider 3 has not secured adequate interconnection capacity with Verizon to handle its traffic, then that congestion may reduce the customer's Netflix streaming speeds. This was precisely the situation earlier in the year as Netflix traffic was sent through peering partners who had failed to obtain interconnection capacity with Verizon adequate to handle the high volumes of traffic they were sending.

⁹ See David Young, *Why is Netflix Buffering? Dispelling the Congestion Myth*, VERIZON POLICY BLOG, <http://publicpolicy.verizon.com/blog/entry/why-is-netflix-buffering-dispelling-the-congestion-myth> (last visited Oct. 27, 2014).

Thus, contrary to Golden Frog's claims, the different Netflix speeds experienced by the FiOS customer with and without the VPN do not "prove" that Verizon was throttling the customer's Netflix traffic, and Verizon did not do so. Instead, the evidence cited by Golden Frog simply confirms that interconnection paths matter, and that the customer experience can be adversely affected where content providers and others do not ensure that they have interconnection capacity capable of handling the volumes of traffic that they direct to another network.

Respectfully submitted,

A handwritten signature in black ink that reads "Roy Litland". The signature is written in a cursive, slightly slanted style.

Roy E. Litland



November 8, 2014

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

Written *Ex Parte* Filing

Open Internet Remand Proceeding, GN Docket No. 14-28; *Framework for Broadband Internet Service*, GN Docket No. 10-127; *Technology Transitions*, GN Docket No. 13-5; *A National Broadband Plan for Our Future*, GN Docket No. 09-51; *State of Wireless Competition*, WT Docket No. 13-135; *Broadband Industry Practices*, WC Docket No. 07-52

Dear Ms. Dortch:

Golden Frog, GmbH submitted Initial comments in the above docket on July 18, 2014. See, e.g., <http://apps.fcc.gov/ecfs/document/view?id=7521709960>. Verizon submitted a letter responding to Golden Frog's comments on October 28, 2014. The letter is available at <http://apps.fcc.gov/ecfs/document/view?id=60000976476>.

Golden Frog addressed Verizon's letter in two "blog" postings. The first is "The FCC Must Prevent ISPs From Blocking Encryption." This was released on November 4. It is publicly available at <http://www.goldenfrog.com/blog/fcc-must-prevent-isps-blocking-encryption>, and a printed version is attached hereto. The blog hyperlinked to two press reports (<https://www.techdirt.com/blog/netneutrality/articles/20141012/06344928801/revealed-isps> and <http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/28/mobile-isp-thwarted-customers-attempts-to-send-encrypted-e-mails-research-finds/>, respectively) that are also reproduced and attached.

On November 6 Golden Frog blogged again. "Hey Verizon, We agree with you," posted on November 6, and available at <http://www.goldenfrog.com/blog/hey-verizon-we-agree-with-you>. The posting is also reproduced and attached. That posting also contained a hyperlink to the previously-mentioned and reproduced Washington Post article.

The blog posts more than adequately respond to Verizon's letter, so further elucidation by counsel is not necessary.

Sincerely,

W. Scott McCollough
Counsel for Golden Frog, GmbH

[Products](#)[Blog](#)[Dump Truck Web App](#)[Control Panel](#)

November 4, 2014

The FCC Must Prevent ISPs From Blocking Encryption

Last month, the popular online publication TechDirt [published an article](#) based on Golden Frog's filing with the FCC that urged the commission to truly restore an Open Internet. A key portion of the article focuses on how we noticed that ISPs and wireless broadband providers can block encryption technologies if they desire.

We discovered this by studying the service of a particular wireless broadband provider, and discovered it was able to interfere with the ability of one of our engineers to encrypt their email communication.

The article gathered a fair amount of attention and we received questions from the press ([including the Washington Post](#)), advocacy groups and our customers. We wanted to share the full story:

A Golden Frog engineer first noticed the issue in September 2013 when he was an AIO Wireless customer. (AIO was a prepaid wireless service provider and subsidiary of AT&T). Being a privacy-focused individual, he set his email client to require using an encrypted connection to his email server using STARTTLS. STARTTLS is an extension to SMTP (the standard email sending protocol) that allows an email server and client to use TLS (Transport Layer Security) to provide private, encrypted, and authenticated communication over insecure Internet connections.

In May 2014, AIO merged with Cricket Wireless so the Golden Frog engineer became a Cricket customer. In June 2014, he brought the issue to the attention of Golden Frog Co-CTO Michael Douglass while the two were working together at a coffee shop. While using his laptop tethered to his phone and connected via Cricket, he was unable to send email securely. He switched to the coffee shop's Wifi and was able to send encrypted email. They concluded that STARTTLS was being intercepted.

The two investigated further and started running tests. They determined Cricket was intercepting and blocking STARTTLS on port 25 – basically, the STARTTLS command was masked out in server responses, and a command failure response was returned. The engineer was connecting to a personal mail server NOT associated with the wireless provider. The test was repeated by connecting to multiple mail servers including Golden Frog's corporate mail servers. These were SMTP connections USING the Cricket/AIO network as a network provider to reach a remote, unaffiliated with AIO mail server.

Golden Frog Co-CTO Philip Molter presented the STARTTLS findings in a lightning talk at the Texas LinuxFest in Austin, TX a couple weeks later. We tested again in July 2014 when we filed our comments with the FCC, and found the same results. We included the screenshots of those test results, which are in [our FCC filing](#).

After the TechDirt article came out, we anticipated we'd get some questions so we ran the same testing and found that STARTTLS is not currently being intercepted and blocked. We are unsure what changed.

We also tested on AT&T's network and found the encryption is not being blocked. Good.

However, this is a clear indication of what wireless ISPs can do under the claim of reasonable network management. Although it has apparently now reversed course, this particular ISP was putting its customers at serious risk by inhibiting their ability to protect online communications. We included it in

our filing because as long as the FCC refuses to return to its prior “open access” policies and enable wide competition then it must establish effective rules to prevent both wireless and wireline ISPs from throttling and blocking users’ Internet traffic and preventing them from using encryption to protect their privacy. We also need more competition between ISPs so if an ISP blocks encryption citizens can “fire their ISP” and choose an ISP that doesn’t block encryption or intentionally slows down content providers such as Netflix.

We ask: Is it reasonable to invade privacy by deactivating encryption to block outgoing spam?

Neither the old or the new proposed Internet rules being debated by the FCC would stop wireless providers from blocking encryption technologies. That is very frustrating and one of the key points in our FCC filing. The FCC is a government organization and tasked with protecting national security when it comes to electronic communications. They are part of the same government that surveils its citizens. It’s not unreasonable to think they are getting pressure to curtail encryption.

Furthermore, ISPs have incentive to block privacy technologies like VPNs. They want to profit as much as possible from the way you use the Internet. Privacy services that are independent of their offerings don’t allow them to do that. If they aren’t selling the service to you, they aren’t making money and that frustrates them. However, when they are blocking privacy services, they are dangerously putting businesses’ confidential communications and individual customers’ privacy at risk.

We strongly believe that the same Open Access rules that should apply to wired Internet providers should also apply to mobile Internet providers, especially considering this specific encryption-related incident that affects online privacy.

[0 Comments](#)

Submit a Comment

Name (required)

Email (required)

Your Comment

Submit



November 6, 2014

Hey Verizon, We agree with you.

In July 2014, Golden Frog filed comments to the FCC in support of Open Access. We included some specific examples:

1. A VyprVPN customer told us he gets better Internet performance with VyprVPN than though his Internet Access Provider (in this case Verizon FIOS).
2. A wireless ISP was blocking a Golden Frog employee's ability to encrypt his communications with his third-party email server. We noted that neither the prior or proposed FCC rules prevent "wired" and "wireless" broadband Internet Access Providers from blocking encryption technologies if they desire.

The strong support our filing received from public advocacy groups and the press' interest in how our product can help alleviate Internet traffic congestion has caused Verizon to [respond to our comments](#).

Surprisingly, we agree with much of what Verizon says.

We never accused Verizon of blocking encryption. As the [Washington Post noted](#), Cricket is the wireless provider that was blocking encryption technologies. However, our point to the FCC is that Verizon (or any other Internet Access Provider) are free to block encryption technologies if they want, and Cricket did so for a while. Encryption inhibits the ISPs abilities to inspect and shape traffic, insert ads and sell additional services. Given their track record, we don't trust the Internet Access Providers and without clear rules at least some will be unable to resist the urge to block or interfere with technologies that inhibit their ability to make money, even if it hurts their customers' privacy.

Customers have noticed better Netflix performance by using our VyprVPN service. One reason is that Golden Frog manages its traffic so it goes to Internet Access Providers over uncongested links. This dramatically improves performance. Verizon agrees that is what is going on here. We won't speculate on how Netflix and others manage their deals with Verizon, but we have been able to provide excellent performance without having to pay Verizon like Netflix did. **We actively manage our network and take it as a compliment that Verizon validated what we do is working.** Congestion is a problem the FCC should fix, but until it does we are providing a workaround for ISPs' tactics.

Verizon's response spoke to "congestion" on the Internet-facing side, but it conspicuously failed to address several other points we made about Verizon's practices on the "user-facing" side. For example, Verizon did not deny that it inspects unencrypted traffic that comes from or goes to its users. Nowhere does Verizon deny that it looks at the content of its own users' Internet communications when it can. Verizon did not deny that it sometimes uses its knowledge of the content for its own advantage or discloses it to others, including the government. Nor did Verizon deny that it performs application identification and then unilaterally applies "special treatment" to some applications – either slowing or assigning priority using as-yet unknown criteria – on unencrypted traffic.

Golden Frog's mission is to provide tools that protect online privacy and provide a truly open Internet around the world. However, VyprVPN has another benefit – it defeats ISP throttling and congestion by application identification and "special treatment." VyprVPN, in effect, becomes the customer's virtual ISP and allows users to benefit from VyprVPN's encrypted connection by boosting their speeds. VyprVPN frustrates the Internet Access Providers' efforts on both the "Internet facing side" and "user-facing side," and simultaneously protects user privacy. **The FCC must act to protect users' continued ability to**

employ options like VyprVPN. If reasonable rules are not put in place Internet Access Providers will expand their monitoring, throttling and blocking and they soon may proceed to prevent users from defending their privacy using encryption tools like VyprVPN.

We strongly urge the FCC to put enforceable rules in place to prevent Internet Access Providers from being able to block VPNs, proxies and other encryption technologies. If the FCC imposes no effective rules against it and the ISPs get their way, poor Netflix performance may be the problem of today, but loss of tools to protect online privacy and security will become tomorrow's problem.

[0 Comments](#)

Submit a Comment

Name (required)

Email (required)

Your Comment

Submit



Insider Shop

Insight Community

Step2

Search Techdirt

Search

Techdirt Wireless News Innovation Case Studies Startups Net Neutrality

Preferences Register Sign In

Main Submit a Story RSS

<< How Australia's New 'Anti-Terror' Censorship...
<< President Obama Makes Vague Meaningless...



NSA Finally Releases Keith Alexander's... >>
FCC Used Title II To Fine AT&T For SMS... >>

Revealed: ISPs Already Violating Net Neutrality To Block Encryption And Make Everyone Less Safe Online

from the *scurry-news* dept

(Mis)Uses of Technology

by Mike Masnick

Mon, Oct 13th 2014 10:38am

0

Filed Under: encryption, fcc, net neutrality, open internet, privacy, security, vpns, vypervpn

Companies: golden frog

Permalink.

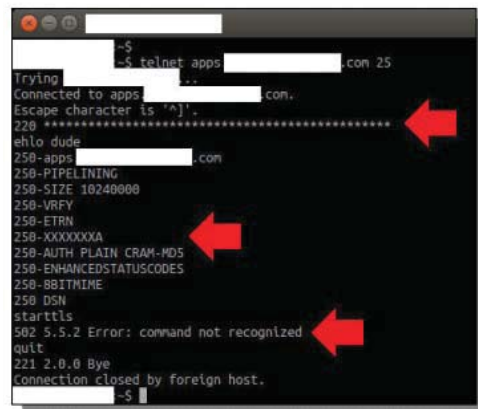
One of the most frequent refrains from the big broadband players and their friends who are fighting against net neutrality rules is that there's no evidence that ISPs have been abusing a lack of net neutrality rules in the past, so why would they start now? That does **ignore** multiple instances of violations in the past, but in combing through the comments submitted to the FCC concerning net neutrality, we came across one very interesting one that actually makes some rather stunning revelations about the ways in which ISPs are **currently** violating net neutrality/open internet principles in a way designed to **block encryption** and thus make everyone a lot less secure. The **filing comes from VPN company Golden Frog** and discusses "two recent examples that show that users are **not** receiving the open, neutral, and uninterrupted service to which the Commission says they are entitled."

The first example you may have actually heard about. It got some attention back in July, when entrepreneur Colin Nederkoorn **released a video** showing how Verizon was throttling his Netflix connection, which was made obvious when he logged into a VPN and suddenly his Netflix wasn't stuttering and the throughput was much higher. That video got a lot of attention (over half a million views) and highlighted the nature of the interconnection fight in which Verizon is **purposely allowing Netflix streams** coming via Level 3 to clog. As most people recognize, in a normal scenario, using a VPN should actually slow down your connection somewhat thanks to the additional encryption. However, the fact that it massively sped up the Netflix connection shows just how much is being throttled when Verizon knows it's Netflix traffic. Nederkoorn actually was using Golden Frog's VyprVPN in that video, so it actually makes Golden Frog look good -- but the company notes that it really shows one way in which "internet access providers are 'mismanaging' their networks to their own users' detriment."

But the second example Golden Frog provides is much scarier and much more pernicious, and it has received almost no attention.

In the second instance, Golden Frog shows that a wireless broadband Internet access provider is interfering with its users' ability to encrypt their SMTP email traffic. This broadband provider is overwriting the content of users' communications and actively blocking STARTTLS encryption. This is a man-in-the-middle attack that prevents customers from using the applications of their choosing and directly prevents users from protecting their privacy.

They demonstrate this with the following graphic:



This is *scary*. If ISPs are actively trying to block the use of encryption, it shows how they might seek to block the use of VPNs and other important security protection measures, leaving all of us less safe. Golden Frog provides more details of what's happening in this case:

Follow Techdirt

Advertisement

Essential Reading

Hot Topics

- 5.7 Lena Dunham Once Again Threatens Lawsuit Over An Interpretation Of Her Book That She Doesn't Like
- 5.6 Former NSA Lawyer Says Reason Blackberry Failed Was 'Too Much Encryption' Warns Google/Apple Not To Make Same Mistake
- 5.6 Guy Accused Of Operating Silk Road 2.0 Arrested In SF... Just Like The Last One

New To Techdirt?

Explore some core concepts:

Advertising Is Content; Content Is Advertising

How Being More Open, Human And Awesome Can Save Anyone Worried About Making Money In Entertainment

Infinity Is Your Friend In Economics

[read all >](#)

Techdirt Reading List

- Parodies of Ownership: Hip-Hop Aest...
Richard L. Schur (Paperback - Jun 4, 2009)
\$26.58
- On Internet Freedom
Marvin Ammori
★★★★★
- Copyfraud and Other Abuses of Intell...
Jason Mazzone (Hardcover - Oct 5, 2011)
\$16.18
★★★★★
- Hollywood's Copyright Wars: From Ed...
Peter Decherney (Hardcover - Apr 10, 2012)
\$31.05
★★★★★

1 2 3 4 5 >

Get Widget Privacy

amazon.com

Techdirt Insider Chat

Golden Frog performed tests using one mobile wireless company's data service, by manually typing the SMTP commands and requests, and monitoring the responses from the email server in issue. It appears that this particular mobile wireless provider is intercepting the server's banner message and modifying it in-transit from something like "220 [servername] ESMTP Postfix" to "200 *****." The mobile wireless provider is further modifying the server's response to a client command that lists the extended features supported by the server. The mobile wireless provider modifies the server's "250-STARTTLS" response (which informs the client of the server's capacity to enable encryption). The Internet access provider changes it to "250-XXXXXXA." Since the client does not receive the proper acknowledgement that STARTTLS is supported by the server, it does not attempt to turn on encryption. If the client nonetheless attempts to use the STARTTLS command, the mobile wireless provider intercepts the client's commands to the server and changes it too. When it detects the STARTTLS command being sent from the client to the server, the mobile wireless provider modifies the command to "XXXXXXX." The server does not understand this command and therefore sends an error message to the client.

As Golden Frog points out, this is "conceptually similar" to the way in which Comcast was throttling BitTorrent back in 2007 via packet reset headers, which kicked off much of the last round of net neutrality concerns. The differences here are that this isn't about blocking BitTorrent, but encryption, and it's a mobile internet access provider, rather than a wired one. This last point is important, since even the last net neutrality rules **did not apply** to wireless broadband, and the FCC is still debating if it should apply any new rules to wireless.

After reading the Golden Frog filing, the answer should be that it is *absolutely necessary* to apply the rules to wireless, because practices like these put us all at risk by *undermining the encryption that keeps us all safe*. As Golden Frog notes:

*Absent enforceable Commission rules, broadband providers can (and at least one already does) block and discriminate against entirely acceptable Internet uses. In this case, users are not just losing their right to use the applications and services of their choosing, but also their privacy. It is not at clear that this type of encryption blocking would be forbidden for fixed broadband Internet access, under the proposed rules' exception for reasonable network management. This example involves mobile wireless broadband, however, and it is clear that the proposed rules would not prohibit the activity. STARTTLS encryption does not constitute "a lawful website" or "an application[]" that compete[s] with the provider's voice or video telephony services[.]"*¹¹ The proposed rules on their face do not prohibit mobile broadband Internet access providers from blocking user efforts to maintain privacy through encryption.

Furthermore, Golden Frog concludes:

The claim that rules banning blocking and unreasonable discrimination are solutions in search of a problem is flatly wrong. There have been problems in the past and there are problems now. The proposed rules do not resolve all of the problems identified in the NPRM. Further broadband Internet access providers are still interfering with beneficial and privacy-enhancing applications users want to employ.

This is incredibly important -- just at a time when we need stronger encryption and privacy online, the FCC may undermine it with weak net neutrality rules that allow this type of behavior to continue.

A few months ago, I got into a conversation with a well-known internet entrepreneur/investor, who asked about possible "compromise" rules on net neutrality, suggesting that maybe it's okay to throttle Netflix traffic because there's *so much* of it. He argued that, perhaps there could be some threshold, and if your traffic was above that threshold it's okay to throttle it. After some back and forth, I asked the hypothetical about encryption: what if, at a time when more and more encryption is important, such a rule was in place, and overall encrypted traffic passed that threshold, then suddenly access providers could throttle all encrypted traffic, doing tremendous damage to security and privacy. What I didn't realize was that some access providers are effectively already attacking privacy and encryption in this manner.

To print the document, click the "Original Document" link to open the original PDF. At this time it is not possible to print the document with annotations.

[Get the Insider Chat!](#)

Advertisement

Recent Stories

Thursday

10:41 Verizon Now Pleads For Bogus Net Neutrality Rules Under 706 Promising It Won't Sue This Time, Ignoring That Others Will Sue (5)

Friday

09:34 FCC Tests The Waters On A 'Hybrid' Net Neutrality Solution That Almost Everyone Hates (21)

Thursday

12:52 Verizon: 'Title II Is Not The Answer... Except When It Gives Us Massive Subsidies, Then It's Totally The Answer' (22)

10:28 Both Comcast And Verizon Agree To Pay Millions To Settle Overbilling Claims (29)

Wednesday

13:41 Cricket Revealed As Mobile ISP That Was Blocking Encrypted Emails (21)

10:33 Detailed Report Shows How ISPs Are Making 'Business Choice' To Make Your Internet Connection Terrible (31)

06:18 Verizon Launches Tech News Blog... That Bans Any Articles About Net Neutrality Or Government Surveillance (33)

Tuesday

13:38 FTC Sues AT&T For Selling 'Unlimited' Data Plans That Were Actually Throttled (18)

Monday

12:16 Payment Wars: How Merchants And Carriers Are Trying To Block Payment Systems They Can't Track (79)

Tuesday

13:45 FCC Used Title II To Fine AT&T For SMS Cramming And The World Didn't End: Why Would It For Broadband? (11)

[More](#)

Advertisement

Ad

The Switch

Mobile ISP Cricket was thwarting encrypted emails, researchers find



By **Nancy Scola** and **Ashkan Soltani** October 28

Follow [@nancyscola](#)

(Courtesy Cricket Wireless)

Some customers of popular prepaid-mobile company Cricket were unable to send or receive encrypted e-mails for many months, according to security researchers, raising concerns that consumers may find that protecting their privacy is not always in their hands.

The inability to send some encrypted messages on Cricket's network was discovered by software engineers from the digital security and privacy firm Golden Frog. The company mentioned the issue in [a July filing to the Federal Communications Commission](#), and [the tech publication Techdirt published an article](#) on it earlier this month. But neither Golden Frog's filing nor Techdirt named the mobile Internet service provider.

Advertisement

Golden Frog told The Washington Post that Cricket customers were unable to send encrypted messages and said its testing found that the problem ended shortly after the TechDirt article was published. It is unclear how long or how many customers were affected.

Cricket did not address repeated questions about the issue and did not alert customers, many of whom rely on Cricket as their sole Internet service, that they would not be able to protect their e-mails from prying eyes. AT&T, which absorbed Cricket when it acquired Leap Wireless last spring, did not respond to a request for comment.

Cricket said in a statement to The Post that it "is continuing to investigate the issue but does not intentionally prevent customers from sending encrypted emails."

Digital encryption allows computers — in this case, the mail servers that send and receive e-mails — to speak to each other in code. The service has been under a spotlight lately as consumers have become concerned about protecting the tremendous amount of information they send across digital networks. Encrypted e-mails were, for example, how NSA contractor Edward Snowden first communicated with journalists about the intelligence community's bulk data collection.

Advertisement

The Most Popular All
Over

THE DODO

In simple terms, encrypting an e-mail typically works like this: User X's mail server asks User Y's mail server if it is willing to receive an encrypted, or coded, e-mail. If the server says, "yes," the encrypted version of the e-mail is sent. If the server says, "no," an unencrypted version is sent instead.

But Golden Frog says that in Cricket's case, when the sending e-mail server asked if it might transmit an encrypted e-mail, the network simply scrubbed the request before the receiving mail server had a chance to hear it.

"The server on the other end doesn't realize that it was asked to speak privately. So it doesn't speak privately," said Andrew Appel, chair of the computer science department at Princeton University.

Golden Frog, which sells privacy-focused software that includes an encrypted messaging service, said it discovered the problem because one of its software engineers living in rural Texas relied on Cricket's mobile Internet service. The engineer had configured his e-mail program to allow his e-mails to be sent only if encrypted.

THE TOLEDO BLADE

Woodville residents react to dog's shooting

SALON

We have been stupefied: How Republicans subvert...

Our Online Games

Play right from this page

Spider Solitaire

Genre(s): [Card](#)

Spider Solitaire is known as the king of all solitaire games!

52 card pickup

Genre(s): [Card](#)

Pick up cards as fast as you can!

Tri-Peaks Solitaire

Genre(s): [Card](#)

Reveal cards as you clear your way to the top!

Carniball

Genre(s): [Arcade](#)

This amusment park classic will bring back some joyous memories

When the company noticed that it was not receiving the employee's e-mails, it began looking into why. Golden Frog found that its engineer was trying to send e-mails through a virtual doorway known as Port 25. That portal has been used to send e-mails for years, but some Internet service providers recently began blocking it because they were concerned that it was dominated by spammers. Still, the system is popular among some tech experts, who use it to operate their own mail servers.

Advertisement

Cricket allowed customers to send and receive e-mails through Port 25 software, according to Golden Frog, but stripped the traffic of the encryption request, known as STARTTLS.

It is unclear whether the lack of encryption was limited to this system or how many Cricket customers were affected.

In its FCC filing, Golden Frog said it was concerned that Cricket's practices violated the spirit of net neutrality, or the idea that Internet service providers should allow Internet traffic to move freely across their networks.

"Any time an Internet service provider is interfering with a user's ability to protect their privacy it's very concerning to

us, and to all Internet users," said Sunday Yokubaitis, Golden Frog's president. "If ISPs can force users' choices about encryption, where does that put us?"

Despite law enforcement complaints, consumers are relying more on digital encryption. [Apple](#) and [Google](#) recently moved to encrypt by default more of the services built into the iOS and Android operating systems. Those moves, [the FBI has argued](#), will make it difficult, if not impossible, for law enforcement to do its job.

According to Google -- [which has called unencrypted e-mail](#) "as open to snoopers as a postcard in the mail" -- [about half of the e-mails received through Gmail](#) in October have been encrypted, up from about 30 percent in January.

Tom Lowenthal is the staff technologist at the Committee to Protect Journalists. "It is poor practice and obsolete to send and receive mail without using robust encryption," Lowenthal said. "Journalists who rely upon secure communications, and anyone else who doesn't want their personal messages to become public, should expect their e-mail providers to offer encrypted connections by default."

Advertisement

Cricket was founded in 1999, and its parent company Leap Wireless was acquired by AT&T earlier this year. (AT&T's network, according to Golden Frog, allowed the sending of encrypted e-mails.) The Golden Frog engineer first noticed the behavior in September 2013 on a network used by AT&T prepaid phone provider Aio. Cricket replaced Aio as

AT&T's pre-paid service after the acquisition was completed in March, and Golden Frog said the encryption practices continued for prepaid customers. Cricket's data plans start at \$35 a month and do not require a contract.

John Levine is a senior technical adviser to the Messaging, Malware and Mobile Anti-Abuse Working Group, an organization with member companies including Apple, Google and Verizon. While it is unclear whether Cricket intentionally prevented its customers from encrypting e-mails, Levine said, "the result is exactly the same."

More and more people are taking steps to protect themselves from spying eyes, Levine said, "and if you're going to interfere with that, you need a really good reason."

Nancy Scola is a reporter who covers the intersections of technology and public policy, politics, and governance.

The NSA has an electronic dragnet. The SEC wants an “agency exception” to the need for a warrant to obtain stored electronic data so they can more easily administer their civil enforcement duties. The Healthcare.gov website requires users to supply sensitive private information before the user can determine eligibility or shop for insurance plans, and this information is shared with a host of other federal agencies and can be used for virtually any purpose. Despite recent revelations about abuse, the IRS is now in charge of receiving and safeguarding more private information, and for more programs, than ever before. The Consumer Financial Protection Bureau is trying to make financial institutions disclose sensitive user transaction and purchasing history. The list goes on. Through these efforts the government is surreptitiously or publicly expanding its surveillance of US citizens in many ways, and trying to extensively gather private information that has historically been out of its reach except through a criminal warrant or voluntary, knowing disclosure. The government often goes to private third party service providers to obtain individuals’ customer data, transactional data and even content, rather than going to the individual. This all-encompassing Big Government/Big Data¹ mining must stop. Individually and collectively these efforts give rise to police-state concerns; they threaten individual liberty and property and violate the Constitution.

Two examples of the government’s hunger for intelligence on its own citizens have received the most discussion: NSA’s activities and the effort by federal regulatory agencies to obtain content from service providers for civil enforcement purposes. While this paper will address only these two, similar concerns arise from other efforts as well.

Most of the commentators addressing the recent revelations of cybersurveillance by the NSA and other entities have focused on whether mass/bulk collection of users’ communications-related information (both “metadata”² and/or content³) violates the Fourth Amendment prohibition of “unreasonable searches and seizures” and its requirement that no “warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or

¹ Those who believe in a limited government should contemplate the proposition that in order for big government to operate with any kind of effectiveness it must have big data.

² The term “metadata” is not defined in any relevant statute. Some have described “telephony metadata” as including “comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call.” “Internet metadata” has included “digital network information” such as connect times, email addresses and IP numbers, among other things. But there is no comprehensive explanation of what “metadata” is and is not. If one were to search for a statutory root for what has been described to date then “telephony” and “Internet” “metadata” information would be a combination of the data covered by 50 U.S.C. 1842(d)(2)(C)(i)(III), (V) and (VI) and (i)(III) and the information gleaned from a “pen register” and/or “trap and trace” authorized in 50 U.S.C. 1805(i), 1842(d)(2)(A)(iii), 1842(d)(2)(C)(i)(III), (V), (V) and 1842(d)(2)(C)(ii)(III). Note that under 50 U.S.C. 1812 the government may also independently obtain information under Title 18 chapters 119, 121, and 206. Those authorities contain roughly synonymous definitions with regard to this issue. *See, e.g.*, 18 U.S.C. 2703(c)(2)(C) and (E) and 18 U.S.C. 3127(3) and (4).

³ 18 U.S.C. 2710(8) defines “contents” to mean “any information concerning the substance, purport, or meaning” of a communication.

things to be seized.” Mass/bulk collection has significant Fourth Amendment implications, but there are other as-yet ignored Constitutional issues.

Similarly, the ongoing efforts to update the Electronic Communications Privacy Act so it better reflects current technology, services and expansion of “the cloud” have hit a snag: several federal agencies, led by the Securities and Exchange Commission, want the ability to directly obtain the content of users’ communication from service providers in the civil context, without any showing of probable cause that a crime has been committed and without having to meet basic Fourth Amendment “particularity” requirements concerning the place to be searched and the things to be seized. Many others have opposed these efforts, and Data Foundry agrees with them. But once again, another set of important Constitutional issues have been overlooked in the debate.

**USERS’ DIGITAL CONTENT IS “PROPERTY” PROTECTED BY THE
FIFTH, NINTH, AND TENTH AMENDMENTS; THERE ARE FIRST AND
SECOND AMENDMENT ISSUES AS WELL**

The ability to own property and exercise the bundle of rights that comes with a property interest is one of the fundamental ways our society exercises liberty. The Fifth Amendment provides that no person may be “deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.”

A “property right” carries with it the right of dominion. It is the right, which a person has, as against all others, to the exclusive control, use, and enjoyment of any particular thing. This includes acquisition and disposal, the right to exclude others, a right against trespass and a right of quiet enjoyment. Interference with this right of dominion over personal property constitutes a trespass to chattel,⁴ and can be a conversion under certain circumstances. The interference need not completely destroy exclusivity in order to be actionable.

⁴ The government may make a copy without consent or require that a copy be made by a third party bailee. Even if the original remains in place a nonconsensual duplication of the original is an exercise of dominion. For example, making a digital copy of the original is an infringement (akin to a taking) on the user’s property rights in the intellectual property realm. Further, it is a trespass to chattel since there is a physical touching of the property, albeit in electronic form, as a necessary prerequisite to making the copy or otherwise obtaining the information. See *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1021 (SD Ohio 1997); *Intel Corp. v. Hamidi*, 94 Cal. App. 4th 325 (Cal. App. 3d Dist. 2001); *Thrifty-Tel, Inc. v. Bezenek*, 46 Cal. App. 4th 1559, 1566, n. 6, 54 Cal. Rptr. 2d 468 (1996); Restatement (Second) of Torts §217b and Comment e, (1963 and 1964) [trespass to chattel includes the intentional use or “intermeddling” with a chattel in the possession of another].

Users' digital content is property.⁵ If you take a picture with a digital camera you own the resulting image file, just as you would an old-style Polaroid. If you do your diary using Microsoft Word[®] the electronic document is the modern equivalent of "papers", just as it would be if you had handwritten the words on paper and placed the book in a secure location in your house. No one would seriously contend that the government can forcibly or surreptitiously enter your home or place of business and seize the digital content (for example, document or image files) on your computer hard drive. Nor would anyone legitimately assert that the government can cut a lock off of a storage unit or safety deposit box you have rented from a third party and confiscate or copy all of the digital files that may have been placed in the rented space. If you are transporting computer disks from your home to the storage using your truck the government cannot just stop the vehicle, rummage through it and traipse away with the disks and information. The government cannot lawfully conceal itself in your house, truck⁶ or rental unit and make a surreptitious digital copy⁷ so as to listen in – unless it meets constitutional due process and probable cause requirements.

In today's world, "the cloud" is the equivalent of a storage unit. The Internet is the equivalent of the road, and electronic communications are modern day conveyors of

⁵ The courts have recognized this property interest, and the legal protection that flows therefrom: "Like the tort of trespass, the Stored Communications Act protects individuals' privacy and proprietary interests. The Act reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility. Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents, *cf.* Prosser and Keeton on the Law of Torts § 13, at 78 (W. Page Keeton, 5th ed. 1984), the Act protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility." *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072-1073 (9th Cir. Cal. 2004).

⁶ See, e.g., *U.S. v. Jones*, 132 S.Ct. 945, 950, n. 3 (2012) (emphasis added):

Justice Alito's concurrence (hereinafter concurrence) doubts the wisdom of our approach because "it is almost impossible to think of late-18th-century situations that are analogous to what took place in this case." *Post*, at ___, 181 L. Ed. 2d, at 928 (opinion concurring in judgment). But in fact it posits a situation that is not far afield--a constable's concealing himself in the target's coach in order to track its movements. *Ibid.* There is no doubt that the information gained by that trespassory activity would be the product of an unlawful search--whether that information consisted of the conversations occurring in the coach, or of the destinations to which the coach traveled. In any case, it is quite irrelevant whether there was an 18th-century analog. Whatever new methods of investigation may be devised, our task, at a minimum, is to decide whether the action in question would have constituted a "search" within the original meaning of the *Fourth Amendment*. Where, as here, the Government obtains information by physically intruding on a constitutionally protected area, such a search has undoubtedly occurred.

⁷ Trespassing and then making a copy without permission clearly interferes with the owner's possessory interest. See *Jones*, 132 S.Ct. 951: "...a seizure of property occurs, not when there is a trespass, but "when there is some meaningful interference with an individual's possessory interests in that property." *Post*, at ___, 181 L. Ed. 2d, at 927 (internal quotation marks omitted). Likewise with a search. Trespass alone does not qualify, but there must be conjoined with that what was present here: an attempt to find something or to obtain information." See also *Id.* at 953 (stating that seizure or monitoring of "electronic signals" that is not accompanied by a trespass is subject to *Katz* "expectation of privacy" analysis, but reserving question on result if there is a trespass on an "electronically signaled" "effect." See also 132 S.Ct. at 955 (Sotomayor, J concurring): "When the Government physically invades personal property to gather information, a search occurs."

content – the truck on the road to the storage unit. The user and the cloud storage providers have a bailor/bailee relationship. The user (bailor) does not waive any property interest. The cloud storage provider (bailee) has the right, indeed perhaps even the duty, to protect the information/property from governmental intrusion.⁸

The government's vast domestic electronic surveillance and the SEC's efforts to have an "agency exception" threaten individual liberty and property, and are contrary to constitutional principles. They erode privacy, impede legitimate business activities, have led to immense domestic and international economic impacts and are wholly antagonistic to the founders' intent and vision.

Data Foundry agrees that information content is the modern manifestation of the "papers and effects" protected by the Fourth Amendment. But it is also "property" for purposes of the Fifth, Ninth, and Tenth Amendments. Surveillance and seizure of digital information also implicates several aspects of the First Amendment, and it could impact the Second Amendment as well. Each of these Amendments form the basis of the "zones of privacy" held by all citizens, including business,⁹ as against any governmental intrusion or confiscation. The "right" to "privacy" directly derives from *property* concepts.¹⁰ This necessarily means the government may not seize digital property without due process of law and just compensation.

⁸ A bailee has the right – and often the duty – to exclude others from possession of the property entrusted to him. See generally Dobie, *Handbook on the Law of Bailments and Carriers* § 61, at 133 (1914) (right); *id.* § 65, at 157-58 (duty); Story, *Commentaries on the Law of Bailments* § 422a, at 421 (4th ed. 1846) (right); *id.* § 457, at 465-66 (duty). "As to everybody except the true owner of" the bailed property, the bailee "has the right of the owner to have and defend its custody and direct possession." See generally 4 LaFave, *Search and Seizure* § 11.3(f), at 344 (2d ed. 1987) ("person who is not the owner of the container but who possesses it by virtue of his status as bailee certainly has standing to object to illegal interference with his possessory interest"). *Foulke v. New York Consolidated Railroad Co.*, 228 N.Y. 269, 275, 127 N.E. 237 (1920). Further, the bailee, whether gratuitous or for hire, has some duty of care. See, e.g., *Voorhis v. Consolidated Rail Corp.*, 60 N.Y.2d 878, 879, 470 N.Y.S.2d 364, 365, 458 N.E.2d 823 (1983) (gratuitous bailee must avoid gross negligence; gross negligence presumed from nonreturn of property); *Aronette Manufacturing Co. v. Capitol Piece Dye Works, Inc.*, 6 N.Y.2d 465, 468, 190 N.Y.S.2d 361, 364, 160 N.E.2d 842 (1959) (bailee for mutual benefit must exercise ordinary care).

⁹ Although corporations are not entitled to the constitutional protections accorded to "citizens" they are "persons" for many (albeit perhaps not all) of the liberty protections afforded by the Constitution. For example, the U.S. Supreme Court long ago held that corporations and businesses are entitled to the procedural and substantive due process protections of the Fifth and Fourteenth Amendments. *Sinking Fund Cases*, 99 U.S. 700, 719 (1879); *Smyth v. Ames*, 169 U.S. 466, 522, 526 (1898); *Grosjean v. American Press Co.*, 297 U.S. 233, 244 (1936) ["a corporation is a 'person' within the meaning of the equal protection and due process of law clauses]. See also *Citizens United v. Federal Election Commission*, 558 U.S. 310, 342-356 (2010) (reaffirming that corporations entitled to First Amendment free speech protection, and overruling recent contrary holdings).

¹⁰ See, e.g., *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) (citations omitted):

Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society. One of the main rights attaching to property is the right to exclude others, . . . and one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of this right to exclude.

- Fifth Amendment. The Fifth Amendment prohibits deprivations “of life, liberty, or property, without due process of law”; “nor shall private property be taken for public use, without just compensation.” This Amendment ensures that citizens have a right to procedural and substantive “due process” as against the federal government in the civil context. It is a “taking” when a governmental entity captures a digital copy of user content while in transit on the Internet, or somehow acquires it while in storage. The user has a right to civil and/or criminal due process and must receive just compensation for the confiscation since the government has effectively deprived the user of his or her property or at least the exclusive right of dominion over and use of it.
- Ninth Amendment. The Ninth Amendment was inserted to re-emphasize the founders’ desire for a federal government with limited scope and to make clear that all powers not granted were withheld by the people and reserved to them. The Ninth Amendment has been characterized as a “constitutional ‘saving clause’”¹¹ This Amendment forms one of the so-called “penumbral” sources of a Constitutional right to privacy.¹² The framers might not be able to understand the technology behind the government’s ongoing domestic surveillance and its efforts to avoid due process and compensation for taking digital property, but they could surely recognize its implications. Although there may be some statutory basis to some extent, nothing in the Constitution expressly authorizes or even contemplates this exercise of power in the absence of war or domestic insurrection, and this is especially so when most of the domestic information captured in the government’s vast surveillance net has no relationship to terrorism or international intrigue, and usually not to any crime. It is a classic case of overbreadth. Similarly, the effort to secure an “agency carve-out” that would allow an agency to seize digital property held by third party bailees over the objection of the bailor who owns the property cannot be squared with any power granted to the federal government. Both efforts are barred by to the Ninth Amendment.
- Tenth Amendment. Like the Ninth Amendment, the Tenth Amendment was promulgated to make clear that the federal government has only those powers expressly granted elsewhere in the Constitution; all other rights and powers are reserved to the people or (as with the Tenth), the states. Both Amendments in large part represent the constitutional equivalent of the judicial interpretative doctrine of *inclusio unius est exclusio alterius*. But they also have substantive import, particularly when other constitutional interests are involved, such as the Fifth Amendment and the First and Second Amendments (discussed below).¹³ While Congress and the Executive Branch have express powers related to surveillance as it pertains to international matters,

¹¹ *Richmond Newspapers v. Virginia*, 448 U.S. 555, 579–80 & n.15 (1980). See also The Rights Retained by the People: The History and Meaning of the Ninth Amendment © George Mason University Press, 1989.

¹² See, e.g. *Griswold v. Connecticut*, 381 U.S. 479, 484-486 (1965); also *Id.* at 487-499 (Goldberg, J concurring).

¹³ See *United States v. Lopez*, 514 U.S. 549, 589, 592-3 (1995) [Tenth Amendment one basis for striking down federal statute outlawing possession of guns in school zone] and *Printz v. United States*, 521 U.S. 898 (1997) [Tenth Amendment prohibits federal statute conscripting state officials into enforcement of federal gun regulatory regime.]

domestic surveillance does not fall within any of the federal governments enumerated powers. Put another way, nothing in the Constitution allows the federal government to engage in cyber-trespassing; it seems beyond peradventure that nothing in the Constitution justifies or allows the federal government engage in secretive trespass and then go on to purloin (through trespass or conversion) citizens' digital property without meaningful due process or any effort to compensate for the property deprivation.

- First Amendment. Government cybersurveillance directly threatens core First Amendment associational and expressive rights. Each person has the right to speak, and to individually decide the audience to whom the person is directly speaking.¹⁴ If the citizen is aware of the monitoring he or she will likely reduce his or her expression and associational activities.¹⁵ Surreptitious monitoring can unlawfully intrude on core expressive and associational rights, including those that have separate Constitutional protection such as the right to bear arms along with other statutory legal protections in the privacy area.¹⁶

CONCLUSION

The government's ongoing efforts to pervasively monitor citizens' through electronic monitoring, interception and by gathering electronic information from third party bailees intrude on individual liberty and property, and violate the Constitution's due process, property, privacy, expression and associational rights. Congress must act before we turn into a full-blown surveillance state.

¹⁴ A person conveying confidential or private information to a chosen recipient cannot have a constitutionally enforceable expectation that the recipient will not further disseminate the message. *See United States v. Miller*, 425 U.S. 435, 433 (1976). But reconveyance by an intended recipient is much different than secret interception by an unknown governmental body during conveyance or surreptitious access to and appropriation of information (property) in storage.

¹⁵ *See Jones, supra*, 132 S.Ct. at 956 (Sotomayor, J concurring):

Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring--by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track--may "alter the relationship between citizen and government in a way that is inimical to democratic society." *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (CA7 2011) (Flaum, J., concurring).

¹⁶ *See* National Rifle Association *amicus curiae* brief, *ACLU, et al v. Clapper, et al*, No. 13-cv-03994 (WHP), S.D.N.Y, Document 44-1 (September 4, 2013).

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)	
)	GN Docket No. 14-28
Protecting and Promoting the Open Internet)	

In the Matter of)	
)	GN Docket No 10-127
Framework for Broadband Internet Service)	

In the Matter of)	
)	GN Docket No. 13-5
Technology Transitions)	

In the Matter of)	
)	GN Docket No. 09-51
A National Broadband Plan for Our Future)	

In the Matter of)	
)	WT Docket No. 13-135
State of Wireless Competition)	

In the Matter of)	
)	WC Docket No. 07-52
Broadband Industry Practices)	

COMMENTS OF i2COALITION

Matthew A. Henry
henry@dotlaw.biz
W. Scott McCollough
wsmc@dotlaw.biz
MCCOLLOUGH|HENRY PC
1250 S. Capital of Texas Hwy., Bldg. 2-235
West Lake Hills, TX 78746
Phone: 512.888.1112
Fax: 512.692.2522

July 15, 2014

EXECUTIVE SUMMARY

The most effective way for the Commission to protect and promote the open Internet is to implement Open Access by reclassifying the broadband transmission component as a Title II telecommunications service. The *NPRM*'s proposed Net Neutrality rules attempt to alleviate the effects of an uncompetitive last mile by regulating broadband access, but Open Access strikes at the heart of the problem by opening up the network to robust competition. Open Access would bring competition back to the Internet access market and consumer choice would be the primary safeguard against abusive and discriminatory network practices.

Open Access was the Commission's prevailing policy for over 40 years. The *Computer Inquiries* laid the groundwork for a vibrant Internet access market and the Commission's policies were successfully adopted around the world. It was not until the Commission abandoned Open Access and broadband competition evaporated that the need for Net Neutrality regulations became apparent. The Commission's decisions to classify broadband as an information service were based on predictions that competition and infrastructure investment would flourish without Open Access. This proceeding provides the Commission the opportunity to reevaluate whether Title I has produced the expected benefits. The evidence is clear that it has not and i2Coalition submits that now is the time to return to Open Access.

If the Commission does not reinstitute Open Access, then it should protect the open Internet with enforceable no-blocking and anti-discrimination rules based on its Title II authority. Section 706 does not provide a solid legal foundation for the Commission's proposed rules and paid prioritization arrangements would be counterproductive. The incredible success of the Internet is largely attributable to the fact that it has always been a level playing field.

Minimal barriers to entry have allowed innovation to come from big and small players alike. However, a bifurcated Internet where the wealthy and powerful can purchase preferential treatment is anathema to the open Internet.

Paid prioritization also presents a dangerous threat to Internet privacy. The only way that broadband access providers can proactively prioritize edge providers' traffic is by monitoring the content of their users' online communications. The Commission should not sanction a prioritization regime that requires Americans to sacrifice their privacy or that allows broadband providers to discriminate against encryption tools.

Protecting the open Internet means establishing meaningful rules that stop discriminatory practices. Open Access, the policy i2Coalition recommends the Commission undertake, would deter abuse through vibrant competition. For 40 years, the Commission's Open Access rules were the foundation of the information services market and they succeeded in fostering competition, preventing discrimination, and incentivizing network investment. These are the results that Commission seeks in this proceeding and it can best achieve them by bringing back Open Access.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	ii
I. DESCRIPTION OF i2COALITION.....	1
II. THERE IS A SIGNIFICANT LIKELIHOOD THAT THE COURTS WILL FIND THE PROPOSED NO-BLOCKING RULE AND COMMERCIALY REASONABLE STANDARD TO BE <i>PER SE</i> COMMON CARRIER REQUIREMENTS.....	1
A. It is very likely that the proposed no-blocking rule will be struck by the courts as a <i>per se</i> common carrier requirement.	3
B. There is a significant likelihood that the proposed commercially reasonable rule will be struck by the courts as a <i>per se</i> common carrier requirement.....	6
C. The Commission should not risk years of regulatory and marketplace uncertainty by implementing rules with dubious legal authority.....	8
III. PAID PRIORITIZATION AND THE COMMERCIALY REASONABLE STANDARD WOULD NEGATIVELY AFFECT EDGE PROVIDERS.....	9
IV. TITLE II RECLASSIFICATION OF THE BROADBAND TRANSMISSION COMPONENT AND REINSTITUTION OF OPEN ACCESS WOULD BETTER PROTECT AGAINST THE HARMS OF AN UNCOMPETITIVE LAST MILE.	11
A. The Commission should acknowledge its prior decisions to close off the network were based on predictive judgments that time has shown were incorrect. The Commission should reverse course and reinstate <i>Computer Inquiry</i> open network principles.....	14
1. Open Access Defined and Contrasted with Net Neutrality.	14
2. Forty years ago, the Commission led the world and created a new Open Access framework.....	17
3. Congress adopted, applied and extended Open Access in the 1996 amendments.	19
4. The Commission serially closed the Open Access network between 1999 and 2007.....	20
5. The Commission also eliminated UNE-based Open Access.	23

6.	Commission predictions that closing the networks would lead to ubiquitous broadband and not threaten the open Internet have proven incorrect.	27
V.	TITLE II RECLASSIFICATION WOULD BE BASED ON THE COMMISSION’S WELL-ESTABLISHED LEGAL AUTHORITY AND WOULD NOT BE SUBJECT TO REJECTION BY THE COURTS.	31
VI.	MOBILE AND FIXED BROADBAND SERVICE SHOULD BE SUBJECT TO EQUAL AND CONSISTENT RULES.	36
VII.	CASE STUDY: PRIVACY AND ENCRYPTION	37
A.	Paid prioritization arrangements are a threat to Internet privacy.	37
B.	The proposed rules fail to account for encryption technologies.	38
VIII.	ANALYSIS OF THE TEXT OF THE PROPOSED RULES	39
A.	Authority for Part 8 Rules	40
B.	Transparency Rule	40
C.	No-Blocking Rule	41
D.	“Commercially reasonable” vs. “No unreasonable discrimination”	42
E.	Other Laws and Considerations	43
F.	§ 8.11 Definitions	43
1.	Definition of “Block” (8.11(a))	43
2.	Definition of “Broadband Internet access service” (8.11(b))	44
3.	Definition of “Edge Provider” (8.11(c))	46
4.	Definition of “Fixed broadband Internet access service” (8.11(e))	46
5.	Definition of “Mobile broadband Internet access service” (8.11(f))	48
6.	Additional Definitions	48
IX.	CONCLUSION	49

I. DESCRIPTION OF i2COALITION

The Internet Infrastructure Coalition (“i2Coalition”) is an industry group that represents the interests of Internet and technology companies on Capitol Hill and before regulatory agencies. i2Coalition believes that an open and free Internet drives economic growth and enhances the lives of people across the United States and around the globe. As an organization, we promote policies that foster continued development and expansion of the Internet. Our members include companies that would fall under the *2014 Open Internet NPRM*’s proposed definition of “edge providers.”¹ In fact, some of i2Coalition’s members were specifically identified as edge providers in the recent *Verizon v. FCC* decision.² i2Coalition’s members have an important interest at stake in this proceeding and we hope to contribute to the Commission’s final rules in a meaningful way.

II. THERE IS A SIGNIFICANT LIKELIHOOD THAT THE COURTS WILL FIND THE PROPOSED NO-BLOCKING RULE AND COMMERCIALLY REASONABLE STANDARD TO BE *PER SE* COMMON CARRIER REQUIREMENTS.

The *NPRM* proposes three enforceable rules to safeguard Internet openness.³ The first is an enhancement of the transparency rule established in the 2010 *Open Internet Order*.⁴ The second is the reinstatement of the no-blocking rule adopted in the *Open Internet Order*, but which was ultimately struck down by the D.C. Circuit in the *Verizon* decision.⁵ The third rule is a prohibition of commercially unreasonable actions that threaten Internet openness. The latter of

¹ *Protecting and Promoting the Open Internet*, Notice of Proposed Rulemaking, 2014 FCC LEXIS 1689 (2014) (“*NPRM*”) at § 8.11(c).

² *Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014).

³ *NPRM* at ¶ 3.

⁴ *Preserving the Open Internet*, Report and Order, 25 FCC Rcd 17905, 17910, ¶ 13 (2010) (“*Open Internet Order*”), aff’d in part, vacated and remanded in part *sub nom.* *Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014).

⁵ *Verizon*, 740 F.3d 623 (D.C. Cir. 2014).

the three is designed to replace the *Open Internet Order*'s anti-discrimination rule and is the primary change of the proposed rules.

The Commission bases its authority to establish these new open Internet rules on Section 706 of the Telecommunications Act of 1996.⁶ The *Verizon* decision held that Section 706 grants the Commission authority to implement rules to protect the open Internet, but struck down the no-blocking and anti-discrimination rules as *per se* common carrier obligations.⁷ The D.C. Circuit reasoned that because the Commission classified broadband Internet access service as a non-common carrier unregulated information service in several decisions between 2000 and 2005, it cannot impose common carrier regulations on broadband Internet access providers.⁸ The Commission has again proposed to use its Section 706 authority to reinstate these rules without undertaking a reclassification of broadband Internet service or its underlying transmission component so as to bring them under Title II. But *Verizon* makes clear that Section 706-based rules will only stand if they do not constitute *per se* common carriage.

When the inevitable appeal of the proposed rules occurs, the reasoning contained in the *Verizon* decision will be applied in the exact same manner. The Commission will return with the same legal authority, an identical no-blocking rule (but with paid prioritization), and a commercial reasonableness standard that is loosely based on the Commission's data roaming rule. The *Verizon* decision provides a clear guide for how the courts will judge the proposed rules and it shows that there is a very good chance the no-blocking rule and the commercially

⁶ Section 706 of the Telecommunications Act of 1996, Pub. L. No. 104-104, § 706, 110 Stat. 56, 153 (1996), as amended in relevant part by the Broadband Data Improvement Act (BDIA), Pub. L. No. 110-385, 122 Stat. 4096 (2008), is now codified in Title 47, Chapter 12 of the United States Code. *See* 47 U.S.C. § 1301 et seq.

⁷ *Verizon*, 740 F.3d at 657-58.

⁸ *Id.*

reasonable standard will be vacated once again because they impose *per se* common carrier obligations and Section 706 does not grant that authority.⁹

A. It is very likely that the proposed no-blocking rule will be struck by the courts as a *per se* common carrier requirement.

The *NPRM* proposes to reinstitute the original no-blocking rule that the D.C. Circuit struck down as a *per se* common carrier obligation.¹⁰ Not one change has been made to the text of the rule.¹¹ As proposed, the no-blocking rule will still require that broadband providers transmit data associated with “lawful content, applications, services, or non-harmful devices” between their customers and edge providers at a prescribed minimum level of service.¹²

The *NPRM* asserts that reintroducing the rule in the same form will not constitute *per se* common carrier regulation this time around because the Commission will allow broadband providers and edge providers to enter into paid priority agreements. The Commission believes that this allowance for individualized bargaining for favored treatment will bring the rule within the Commission’s Section 706 authority because it allows for discriminatory terms, a non-common carrier attribute.¹³

The *NPRM* claims that the *Verizon* ruling invited the reintroduction of the no-blocking rule with permission for broadband providers to negotiate terms for paid priority treatment.¹⁴ Unfortunately, this is an overly-optimistic reading of the ruling and the decision should not be

⁹ i2Coalition believes that the Commission should simply embrace and apply its Title II authority, and then require unbundling and a separate offer of the transmission component by returning to *Computer Inquiry* Open Access. New competitive entry in the Internet access market will then deter the evils identified in the *NPRM*. If the Commission does not return to Open Access then i2Coalition concurs with many of the commentators who recommend reliance on Title II to regulate the currently non-competitive Internet access market through meaningful and effective no-blocking and non-discrimination rules.

¹⁰ *NPRM* at ¶¶ 89-109.

¹¹ The Commission has proposed a new definition for “block” that was absent from the original rules, which contemplates a new “minimum level of access” and performance below that minimum level constitutes a “block.”

¹² *NPRM* at ¶¶ 89-90. .

¹³ *Id* at ¶ 95.

¹⁴ *Id* at ¶ 97.

read with such certitude. The court refused to consider this argument because it was not in the original order or briefed. The portion of the decision the *NPRM* cites as support for the currently-proposed no-blocking rule was instead merely a recitation of the oral argument made by the Commission. At no point does the decision actually state that a no-blocking rule could be implemented under the Commission's Section 706 authority if only it is combined with individualized negotiations for priority. And even if it had, such a statement would have been made without the benefit of briefing. To say the least, the Commission is on very tenuous grounds basing its approach on the belief that this sort of no-blocking rule has already been preapproved in *Verizon*.

The *Verizon* decision shows that this new effort would be analyzed primarily against the Supreme Court's 1979 decision in *Midwest Video II*.¹⁵ Under that precedent the new rule will almost certainly be found to still be a *per se* common carrier obligation.¹⁶ The *Verizon* decision found the *Open Internet Order*'s no-blocking rule to be "indistinguishable" from the no-blocking rule in *Midwest Video II* because both require the regulated entities to carry the content of third parties to their customers. In both cases, the service provider could otherwise block content absent the rule, which, according to the court, effectively transfers control over the transmissions to the third parties.¹⁷ In both *Midwest Video II* and *Verizon*, the no-blocking rule constituted a minimum level of service that third parties received free of charge. Both conditions are common carrier obligations and both remain present in the *NPRM*'s no-blocking rule. This iteration of the no-blocking rule will produce the same Section 706 result as the last iteration and for the same reasons.

¹⁵ *FCC v. Midwest Video Corp.*, 440 U.S. 689 (1979).

¹⁶ *Verizon*, 740 F.3d at 651.

¹⁷ *Id* at 655.

The addition of negotiated, commercially reasonable paid priority service does not change this analysis. Prioritization would be completely separate from the mandatory minimum level of service that constituted *per se* common carriage in *Verizon*. The no-blocking rule sets the floor below which the broadband provider's service cannot fall. Priority treatment, on the other hand, would simply constitute the purchase of adjunct, premium service on top of the minimum level of service. Common carriers have always had the ability to negotiate individual agreements for supplemental and priority services above standard minimum levels of service without affecting common carriage obligations.¹⁸

Nor would the addition of paid prioritization to the non-blocking rule be analogous to the Commission's data roaming rule, which the D.C. Circuit found to be a non-common carrier obligation in *Cellco*.¹⁹ The data roaming rule does not require free access and in fact does not require a minimum level of service at all. The "substantial room for individualized bargaining" central to the data roaming rule is significantly curtailed by the present proposal to impose a no cost "minimum level of service" option for edge providers.²⁰ The no-blocking rule also severely curtails broadband providers' right to "make individualized decisions, in particular cases, whether and on what terms to deal."²¹ Minimum terms are dictated by the Commission and decisions regarding "whether" to serve edge providers are foreclosed. The contemplated option of providing an additional service – presumably for a charge – does not change the fact that the proposed rule would still require a basic service, without any room for negotiations about whether, or on what terms, that service will be provided. This plainly constitutes the imposition

¹⁸ See, e.g., Letter from Robert W. Quinn, Jr., AT&T Services, Inc. to Marlene H. Dortch, Secretary, Federal Communications Commission, GN Docket No. 14-28 (filed May 9, 2014) at pp. 7-8.

¹⁹ See *Cellco P'ship v. FCC*, 700 F.3d 534 (D.C. Cir. 2012).

²⁰ *Id* at 548.

²¹ See *National Association of Regulatory Utility Comm'rs v. FCC*, 525 F.2d 630, 643 (D.C. Cir. 1976) (*NARUC I*); *National Association of Regulatory Utility Comm'rs v. FCC*, 533 F.2d 601, 608-609 (D.C. Cir. 1976) (*NARUC II*).

of *per se* common carriage obligations under *Midwest Video II* and *Cellco* and meets the common carrier attributes set out in *NARUC I* and *II*.

The *Verizon* decision struck down the *Open Internet Order*'s no-blocking rule because it mandated that all edge providers receive a minimum level of access, which is a hallmark of common carriage.²² Allowing the provision of negotiated preferential treatment above this minimum level of service does nothing to actually eliminate the underlying *per se* common carrier obligation. If the *NPRM*'s rules are adopted as proposed, the D.C. Circuit will again apply the *Midwest Video II* holding in the inevitable appeal and the no-blocking rule will almost certainly be struck down for the same reasons it was rejected in *Verizon*.

B. There is a significant likelihood that the proposed commercially reasonable rule will be struck by the courts as a *per se* common carrier requirement.

The *NPRM* has replaced the *Open Internet Order*'s anti-discrimination rule with a general prohibition of commercially unreasonable practices by broadband Internet access providers.²³ This new rule replicates the Commission's *Data Roaming Order* and the attendant data roaming rule in many respects.²⁴ The data roaming rule was held by the D.C. Circuit to not constitute a common carrier obligation because it allowed "substantial room for individualized bargaining and discrimination in terms."²⁵ However, the new commercially reasonable standard significantly expands upon the data roaming rule and may very well be held to include so many marks of common carriage as to be outside the Commission's Section 706 authority.

²² *Verizon*, 740 F.3d at 658-9 ("In requiring that all edge providers receive this minimum level of access for free, these rules would appear on their face to impose *per se* common carrier obligations with respect to that minimum level of service.").

²³ *NPRM* at ¶ 116.

²⁴ *Reexamination of Roaming Obligations of Commercial Mobile Radio Service Providers and Other Providers of Mobile Data Services*, Second Report and Order, 26 FCC Rcd 5411, 5433, ¶ 45 (2011) (*Data Roaming Order*).

²⁵ *Cellco*, 700 F.3d at 548.

The commercially reasonable standards proposed in the *NPRM* go well beyond the scope of the data roaming rule in several important respects. For instance, the data roaming rule imposes an obligation for wireless carriers to undertake commercially reasonable actions in only one situation, namely negotiations over data roaming agreements. The *NPRM*'s commercially reasonable standard, however, would apply to all actions involved in the provision of broadband service.²⁶ This would include relations with customers, network management, and interactions with edge providers.

One aspect that the D.C. Circuit found determinative when holding that the *Data Roaming Order* did not impose common carriage obligations was that the rule includes no presumption of reasonableness.²⁷ The Commission set neither an upper limit nor a lower limit outside of which a data roaming agreement became commercially unreasonable. Instead the Commission left it to the market to determine the range of acceptable terms and rates. The *NPRM*'s commercially reasonable rule does not do this, however. Instead, the Commission presumes that providing the mandatory minimum level of service free of charge to edge providers is reasonable. This sets a floor below which negotiations for priority delivery will never drop.

By imposing a no-blocking rule and a minimum level of free service for edge providers, the Commission is mandating “generally applicable terms” for broadband.²⁸ Every customer will have access to every edge provider and every edge provider will secure unblocked transmission of their traffic free of charge. It is likely that only the largest edge providers will negotiate prioritized treatment and the vast majority will instead make do with the generally

²⁶ *NPRM* at ¶ 116.

²⁷ *Cellco*, 700 F.3d at 550.

²⁸ *Id* at 546 (“[T]he indiscriminate offering of service on generally applicable terms . . . is the traditional mark of common carrier service.”) (quoting *Southwestern Bell Telephone Co. v. FCC*, 19 F.3d 1475, 1481, (D.C. Cir. 1994)).

applicable minimum level of service. Most edge providers will forego negotiations for paid priority treatment for many reasons, including cost and traffic volume. They will accept the minimum level of service available to them. Data roaming, however, cannot occur at all, at any level, until there are negotiations and an agreement. An agreement is a mandatory prerequisite to obtaining access of any kind. In these respects, the *NPRM*'s commercially reasonable rule significantly departs from the *Data Roaming Order*.²⁹

The *NPRM*'s commercially reasonable standard creates substantially less room for individualized bargaining and discrimination in terms than the *Data Roaming Order*. The *Cellco* decision noted that the *Data Roaming Order* "bears some marks of common carriage," but deferred to the Commission because those marks did not so predominate as to relegate wireless carriers to common carrier status.³⁰ By eliminating the mandatory negotiation process, creating a presumption of reasonableness, setting generally applicable terms, and proposing to apply the commercially reasonable standard as a general rule for broadband providers, the *NPRM* bears far more marks of common carriage than the data roaming rule. There is a significant likelihood that this expansion of *per se* common carrier obligations will be found to so predominate as to relegate broadband providers to common carriers in violation of the Commission's Section 706 authority.

C. The Commission should not risk years of regulatory and marketplace uncertainty by implementing rules with dubious legal authority.

Section 706 does not provide solid legal authority for the Commission to implement the no-blocking rule and the prohibition on commercially unreasonable practices. The latter is being proposed in order to impose a non-discrimination rule while not calling it common carriage. The

²⁹ *Id* at 546 ("[T]he indiscriminate offering of service on generally applicable terms...is the traditional mark of common carrier service.") (quoting *Southwestern Bell Telephone Co. v. FCC*, 19 F.3d 1475, 1481, (D.C. Cir. 1994)).

³⁰ *Id* at p. 537.

allowance for individually negotiated priority agreements only affects the upper bounds of edge provider access to broadband networks, but leaves the common carrier minimum level of service untouched. Similarly, the significant expansion of the commercially reasonable standard risks so predominating broadband service as to constitute *per se* common carriage. The Commission's efforts bear a very high likelihood that one of the two rules, if not both, will be struck yet again.

Should the Commission's open Internet rules be vacated for a third time, the result will be a decade and a half of market and regulatory uncertainty, as well as a non-neutral Internet. Those are years that the broadband market cannot get back and in which the United States became increasingly uncompetitive with other developed countries. The Commission should not knowingly set out on tenuous legal authority to protect the open Internet. To do so invites legal challenge and forecloses the type of certainty that businesses and investors require. This is especially unwise when the Commission plainly has the ability to accomplish the same policy objectives on well-established, indisputable legal authority under Title II.

III. PAID PRIORITIZATION AND THE COMMERCIALLY REASONABLE STANDARD WOULD NEGATIVELY AFFECT EDGE PROVIDERS.

The *NPRM* has proposed to replace the *Open Internet Order*'s anti-discrimination rule with a commercially reasonable standard and permission for broadband Internet access providers to enter into negotiated paid prioritization agreements with edge providers.³¹ The Commission believes that the combination of these two changes brings the proposed rules within the Commission's Section 706 authority.³² These rules, therefore, were not developed and proposed for the positive benefits they would bring consumers, but rather as jurisdictional hook.

³¹ *NPRM* at ¶¶ 97 and 110.

³² *Id* at ¶ 118.

Paid prioritization on the last mile is a significant and unnecessary change to the way that Internet access has traditionally been provisioned. Allowing edge providers to purchase preferential treatment, and therefore a higher-quality connection to end users, dramatically changes one of the Internet's most beneficial features; the level playing field. The Chairman's statement is adamant that prioritization will not lead to a fast lane-slow lane dichotomy.³³ However, bandwidth is a zero-sum resource. Any increase in the share of bandwidth to certain edge providers necessarily reduces the share available to the non-favored edge providers.

A paid prioritization regime will benefit broadband access providers and established edge providers, but hurt small edge providers, competition, innovation, and ultimately consumers. Preferential treatment for those edge providers that can afford premium service provides a competitive advantage against all non-prioritized edge providers. In a paid priority system, wealthy edge providers will be able to prevail over competitors by out-spending them, rather than by creating superior products. This will further entrench the established and presently-successful edge providers at the expense of new and small competitors. Start-ups that require priority service may not be able to bring their product to market without significant outside investment and investors will be affected by the increased equity needs of entrepreneurs. All of these negative effects are incompatible with the concept of an open and dynamic Internet. Instead, a prioritized Internet is one that favors the status quo over innovation and change.

The commercially reasonable standard also threatens to further entangle unregulated edge providers in the Commission's regulatory regime. The *NPRM* proposes to enforce the commercially reasonable standard through the Commission's formal complaint process.³⁴ This means that the Commission is delegating watchdog responsibilities to edge providers with no

³³ *Id.* at pp. 86-88.

³⁴ *Id.* at ¶ 172.

experience with the Commission or its rules. The prospect of hiring attorneys to litigate a potentially years-long formal complaint at the Commission whenever faced with an unreasonable practice is an incentive *not* to venture into the edge provider business.

Paid prioritization and a complaint-based commercially reasonable standard do not advance the open Internet. Instead these factors water-down the *Open Internet Order's* anti-discrimination rule in order to sustain a claim to Section 706 authority. However, this is entirely unnecessary because Title II authority is indisputably available to the Commission.

IV. TITLE II RECLASSIFICATION OF THE BROADBAND TRANSMISSION COMPONENT AND REINSTITUTION OF OPEN ACCESS WOULD BETTER PROTECT AGAINST THE HARMS OF AN UNCOMPETITIVE LAST MILE.

The fundamental dilemma that the Commission faced with the Internet Policy Statement, in the *Open Internet Order*, and which it faces in this proceeding is that it wants to impose a common carrier principle upon non-common carriers. “Net Neutrality” is a euphemism for the combination of common carrier prohibitions against blocking and discrimination.³⁵ Twice the Commission has failed to lawfully impose Net Neutrality obligations on unregulated broadband providers, yet it is once again attempting to fit a square peg in a round hole. Instead, the Commission should reclassify the transmission component of broadband Internet access and open it up to competition. In other words, bring back Open Access.

The need for Net Neutrality regulations arises entirely because predecessor Commissions between 1999 and 2007 allowed telephone and cable companies to close off competitive access to bottleneck broadband infrastructure and services, thereby eliminating broadband Internet

³⁵ The avowed purpose is to prohibit or limit access provider discretion that is inconsistent with user choice or societal goals. i2Coalition agrees that this is necessary precisely because access providers have the incentive and ability to act in ways contrary to the public interest and user choice in many ways and have so acted, just as the Commission has recently recognized. In other words, i2Coalition agrees that blocking and discrimination are evils to be avoided. The point here is that *per se* common carriage through Open Access or some form of Net Neutrality is the only way the Commission can effectively eliminate unreasonable discrimination in access to or the use of broadband transmission.

access competition. Thus, the telephone and cable companies were effectively granted a duopoly over wireline broadband access. Without competition and consumer choice to reign in harmful broadband practices, the Commission has sought to protect American Internet users with Net Neutrality rules for the past nine years.

The Commission has now properly recognized that the duopoly providers have both the incentive and the means to act in ways contrary to the public interest.³⁶ In an effort to rectify these evils, the Commission chose to regulate Internet access providers through Net Neutrality rules, rather than taking the more logical step of re-opening the network by returning to the Open Access rules that allowed the Internet to flourish from the beginning. The Internet developed into an open platform because the essential underlying facilities and services were themselves open to competition. It was the move away from Open Access and competition on the underlying network that ultimately necessitated this *NPRM*.

The Commission's explanation for excluding dial-up Internet access from Title I reclassification the *Open Internet Order* directly illustrates that this is so. The Commission explained that competitive forces and regulation of the underlying transmission component protected dial-up service from monopoly abuses and the *Order's* Net Neutrality rules were therefore unnecessary.

[T]he easy ability to switch among competing dial-up Internet access services. Moreover, the underlying dial-up Internet access service is subject to protections under Title II of the Communications Act. The Commission's interpretation of those protections has resulted in a market for dial-up Internet access that does not present the same concerns as the market for broadband Internet access.³⁷

This statement acknowledges that Open Access and a competitive marketplace is preferable to Net Neutrality rules. If the Commission reinstates Open Access on the last mile transmission

³⁶ *Open Internet Order*, 25 FCC Rcd at 17915-928, ¶¶ 20-37; *see also NPRM* at ¶¶ 6, 26, and 39-53.

³⁷ *Open Internet Order*, 25 FCC Rcd at 17935, ¶ 51.

networks, then the underlying concerns will go away and regulation of bundled Internet access services will not be necessary.

The Commission should also determine – now that experience has been gained and lessons learned – that the *Brand X* dissent was right: “the telecommunications component of cable-modem service retains such ample independent identity that it must be regarded as being on offer.”³⁸ The Commission now has the experience to find that a course-reversal is indicated and the transmission component *can and should be* regarded as a separate offering. The transmission component should be isolated and brought back under Title II. The Commission will then have firm ground upon which to rest its rules preventing the evils that have been identified in the *NPRM*.

i2Coalition suggests that the Commission does not have to directly regulate the bundled Internet access product. That product can plausibly remain an unregulated, non-common carrier information service – even when offered by the infrastructure owner or an affiliate – so long as the transmission component is available to unaffiliated parties on just, reasonable and non-discriminatory terms, equal to those applicable its affiliate. While i2Coalition believes that structural separation is preferable, it is not mandatory. Nonstructural safeguards can be crafted that would allow the infrastructure owners to offer the bundled information service if the underlying transmission is available to others on an unbundled basis.³⁹

³⁸ *Nat’l Cable & Telecomms. Ass’n. v. Brand X Internet Servs.*, 545 U.S. 967, 1008 (2005) (Scalia, J., dissenting).

³⁹ If the Commission chooses the incongruous course of keeping the network closed while trying to still save the open Internet, and proceeds to regulate the Internet access output, then bringing the transmission component within Title II is still a necessary legal foundation because all of the potential alternatives constituting effective and enforceable remedies will meet the test for *per se* common carriage. The Commission should include Title II as a basis for the rules that emerge from this proceeding.

- A. The Commission should acknowledge its prior decisions to close off the network were based on predictive judgments that time has shown were incorrect. The Commission should reverse course and reinstate *Computer Inquiry* open network principles.**

The D.C. Circuit's *vacatur* of the nondiscrimination and no blocking rules provides an opportunity for the Commission to once again embrace and preserve Open Access, which is a preferable and less intrusive way to ensure an open Internet in the United States.

1. Open Access Defined and Contrasted with Net Neutrality.

There is a significant difference between "Open Access" and "Net Neutrality" as that phrase has been applied in the United States. Whereas Open Access creates alternatives to cable- or telco-affiliated ISPs at the physical and logical layer, Net Neutrality focuses on protecting competition at the application and content layers. Net Neutrality is a remedy for evils that arise in the absence of Open Access and competition in the broadband marketplace.

The Commission unwisely abandoned Open Access when it closed off competition on the transmission facilities deployed by the incumbent telephone and cable companies. This about-face from the Open Access policies established in the *Computer Inquiry* trilogy⁴⁰ began in the late 1990s and has continued to date, through a series of cases restricting enhanced/information service providers' ability to obtain access to infrastructure – both directly and through

⁴⁰ *Regulatory and Policy Problems Presented by the Interdependence of Computer and Communication Service Facilities*, Notice of Proposed Rulemaking and Tentative Decision, 28 F.C.C.2d 291 (1970), Final Decision and Order, 28 F.C.C.2d 267 (1971) (*Computer I*), *aff'd in part sub nom. GTE Service Corp. v. FCC*, 474 F.2d 724 (2nd Cir. 1973), *decision on remand*, Order, 40 F.C.C.2d 293 (1973); *Amendment of Section 64.702 of the Commission's Rules and Regulations*, Tentative Decision, 72 F.C.C.2d 358 (1979), Final Decision, 77 F.C.C.2d 384 (1980) (*Computer II*), *recon.*, Mem. Op. and Order 84 F.C.C.2d 50 (1981), *further recon.*, Order on Further Reconsideration, 88 F.C.C.2d 512 (1981), *aff'd sub nom. Computer and Communications Industry Ass'n. v. FCC*, 693 F.2d 198 (D.C. Cir. 1982), *cert. denied*, 461 U.S. 938 (1983), *aff'd on second further recon.*, Mem. Op. and Order, 56 Rad. Reg. 2d (P&F) 301 (1984); *Amendment of Section 64.702 of the Commission's Rules and Regulations*, Report & Order, 104 F.C.C.2d 958 (1986), *recon.*, Phase I Reconsideration Order, 2 F.C.C.R. 3035 (1987), *further recon.*, Order on Further Reconsideration, 3 F.C.C.R. 1135 (1988), *second further recon.*, Order on Second Further Reconsideration, 4 F.C.C.R. 5927 (1989), *Report & Order and Phase I Reconsideration Order vacated sub nom. California v. FCC*, 905 F.2d 1217 (9th Cir. 1990), *decision on remand*, Computer III Remand Proceedings: Report and Order, 5 F.C.C.R. 7719 (1990) (*Computer III*).

competitive carriers – and then changing the regulatory classification for broadband Internet access provided by cable, telephone companies, wireless providers, and broadband over powerline.

Past Commissions took these actions despite the fact that the current Communications Act was almost entirely premised on competitive access to unbundled monopoly or duopoly transmission facilities, the epitome of Open Access. Much of the rest of the world followed the original American model and embraced Open Access – probably because the U.S. Government urged them to do so⁴¹ – and they have retained it even after the Commission reversed course. That is one of the major reasons there is far more competition, better and faster Internet capabilities, and lower prices abroad.

There is not a universally-accepted definition of Open Access. The Commission has equated Open Access with multiple-ISP access in the context of cable networks, but the concept of Open Access truly arose in the *Computer Inquiries*. In particular, Open Access was the shorthand term for the ability of unaffiliated enhanced service providers to obtain telecommunications inputs from LECs in the form of “Open Network Architecture” or “ONA.” However, the Open Access concept is not unique to communications. For example, the energy industry still operates under some variants of an Open Access regime.⁴²

For fixed networks, Open Access policies usually take the form of regulated access, such as local loop unbundling, dark, grey and lit fiber and other wholesale access products. These

⁴¹ See Press Release, *United States Urges EU to Continue Progress in Opening Communications Market To Competition*, 2000 FCC LEXIS 1383 (2000), available at http://www.fcc.gov/Bureaus/International/News_Releases/2000/nrin0005.doc (“In order to harness the full power of the Internet, we urge EU Member State regulators to Open Access of local networks to competitive suppliers of Digital Subscriber Lines and other innovative technologies.”).

⁴² See, e.g., *Associated Gas Distributors v. FERC*, 824 F.2d 981, 1007 (D.C. Cir. 1987), *cert. denied*, 108 S.Ct. 1468, 1469 (1988) (upholding FERC authority to establish Open Access for gas transmission); *New York v. FERC*, 535 U.S. 1 (2002) (upholding FERC authority to establish Open Access for electric transmission); *Promoting Wholesale Competition Through Open Access Non-Discriminatory Transmission Services by Public Utilities*, 61 Fed. Reg. 21540 (1996).

products derived capacity such as digital and optical carrier (DSx, OSx), as well as other capacity-based offerings like Ethernet, and can also include next layer (e.g., bitstream) services. Policy makers and regulators in most countries realize that these infrastructure elements represent a major barrier for the entry of alternative ISPs without mandatory access.

Net Neutrality is not Open Access. Indeed, Tim Wu, who is credited with crafting the Net Neutrality concept, took great pains to distinguish Net Neutrality from Open Access in his original paper that introduced the topic.⁴³ Open Access is about opening essential infrastructure to competition. Net Neutrality accepts that there is no Open Access, and regulates Internet access rather than the essential facilities.

The 2005 Commission concluded that retaining Open Access as a regulatory policy would not provide sufficient incentives for the telephone companies and cable companies to invest in broadband transmission.⁴⁴ They underappreciated the fact that eliminating Open Access meant that the incumbents would obtain monopoly control of both the transmission market and the adjacent Internet access market, and both would be susceptible to abuses of market power. The 2010 Commission then applied Net Neutrality as a palliative band-aid to mask the fact that eliminating Open Access removed the possibility for intramodal competition in the Internet access market.

⁴³ Prof. Tim Wu, *Network Neutrality, Broadband Discrimination*, Journal of Telecommunications and High Technology Law, Vol. 2, p. 141 (2003). Available at SSRN: <http://ssrn.com/abstract=388863>. Wu's paper appears to equate "Open Access" with "structural separation." See, e.g., *id.* at 148 ("The term open-access is used in many different ways; it generally refers to a structural requirement that would prevent broadband operators from bundling broadband service with Internet access from in-house Internet service providers.") Open access, however, is possible even in the absence of structural separation. For example, *Computer III* replaced structural separation with accounting safeguards, but retained Open Access. *Computer Inquiry* allowed the incumbents to bundle their own offering, so long as they had an unbundled offering available to third party providers.

⁴⁴ See, e.g., *Appropriate Framework for Broadband Access to the Internet Over Wireline Facilities*, 20 FCC Rcd 14853, 14855, 14860, and 14877-878, ¶¶ 1, 19, and 44 (2005) (*DSL Reclassification Order*).

It is time for the Commission to bring back Open Access and competition in the broadband market. Net Neutrality to date has not cured the disease, and it presents insuperable legal and practical problems.

2. Forty years ago, the Commission led the world and created a new Open Access framework.

Over 40 years ago, the Commission instituted Open Access primarily through the original service unbundling rules established in the seminal *Computer Inquiry* trilogy. Other competition-enhancing efforts dealing with customer premises equipment and inside wiring were adopted by Congress and approved by the courts. All of these actions were based on Open Access concepts. Other federal agencies applied the same concepts to the energy industry, resulting in tremendous competition and consumer benefits.⁴⁵ This set the stage for the explosive growth of the Internet and much of the world followed the Commission's lead.

The *Computer Inquiries'* Open Access model was deregulatory, but did not eschew Title II regulation where widespread competition was not truly feasible. The first step was to isolate monopoly telecommunications components, and impose regulation on the monopoly activity – and that activity only. The regulations made these non-competitive components available to users and potential entrants in order to allow competition to thrive where it was possible.⁴⁶ The

⁴⁵ Electric and gas transmission Open Access has reduced wholesale prices for energy, and the cost reduction input has flowed to retail customers. On the electric side it has much contributed to the growth of solar and wind power as an alternative to carbon fuels and nuclear. The same concept has also directly benefitted retail energy customers, because the principle has also allowed retail customers to “attach” solar and gas self-generation to the electric grid, allowing them to self-generate but also receive standby and back-up and sell excess energy. In many respects this is akin to the original Policy Statement that “consumers are entitled to connect their choice of legal devices that do not harm the network.” *Appropriate Framework for Broadband Access to the Internet over Wireline Facilities*, 20 FCC Rcd 14986, 14988 (2005). Consumer attachment rights arose from *Hush-a-Phone*, *Hush-a-Phone Corp. v. U.S.*, 238 F.2d 266 (D.C. Cir. 1956), and *Carterphone*, *In the Matter of Use of the Carterfone Device*, 13 F.C.C.2d 420 (1968), but the *Computer Inquiries* also advanced attachment rights by deregulating CPE and inside wire while maintaining regulations enforcing the attachment right, including the Part 68 process.

⁴⁶ Although Internet access certainly depends on transmission service inputs, it is not solely raw transmission. Other arguably non-telecommunications functions are sometimes offered along with the transmission. Internet access is a distinct, secondary service that can plausibly be said to reside in an “adjacent” market. The question, however, is whether the bundled output is still telecommunications. If one uses the *Computer Inquiries* parlance, the decision to

second step was to deregulate value-added enhanced service markets that rely on telecommunications inputs, but are not themselves telecommunications *and* can be competitive if bottleneck telecommunications inputs are available on a nondiscriminatory basis.

The *Computer Inquiries* spurred the rise of unregulated value-added networks that had specific rights to access facilities, such as local plant, so they could provide “enhanced services.” Those decisions directly and inexorably led to the rise of the Internet.⁴⁷ The Commission itself – until relatively recently – repeatedly emphasized that the Internet as we know it would not exist but for the *Computer Inquiry* Open Access rules.⁴⁸

be made depends on whether the telecommunications component is “contaminated” by and subsumed within the bundled output. That is the basic perspective used in the *Cable Modem Declaratory Ruling* and then leveraged into the *DSL Reclassification Order*. A correct application of the *Computer Inquiries* would have resulted in application of “adjunct to basic” rather than “contamination” to most of the major providers since they were carriers and facilities-based. The Commission long ago explained – for good reason – that the contamination doctrine cannot and should not be used for facilities-based entities that engage in common carrier activity. See *IDCMA Frame Relay*, Memorandum Opinion & Order, 10 FCC Rcd 13717, 13719-720, and 13723-24, ¶¶ 17-18 and 42-45 (“AT&T cannot avoid its *Computer II* and *Computer III* obligations under the auspices of the contamination doctrine, which applies only to nonfacilities-based service providers”). As we explain below, the Commission should have used “adjunct to basic” for the preponderance of cable modem providers, all of the major DSL providers and even the broadband wireless providers that are CMRS because they were in fact common carriers, at least in part, and they are facilities-based.

⁴⁷ The entities the *NPRM* labels edge providers are predominately non-carriers, and most do not own extensive transmission networks. Some do have some privately-owned transmission, but they still much resemble the “Value Added Networks” discussed in *Computer Inquiry* although their primary function is no longer protocol conversion. All exist entirely as a result of *Computer Inquiry* because that set of proceedings ensured these entities would have Open Access to bottleneck transmission and would not suffer unnecessary regulation.

⁴⁸ A fine collection of such observations appears in *The FCC and the Unregulation of the Internet*, FCC OPP Working Paper, July 31, 1999, available at http://transition.fcc.gov/Bureaus/OPP/working_papers/oppwp31.pdf:

Open access across the telecommunications network has driven the deployment of innovative and inexpensive Internet access services. ... the growth and continued success of the Internet, and the ability of market forces to sustain and encourage that growth, can be attributed to one basic attribute: the openness of both the Internet and the underlying telecommunications infrastructure. ... To the extent that the Internet has relied on the openness of this nation’s communications infrastructure to reach all corners of this nation, this ingredient in its success has not been an accident. The FCC has taken numerous steps since the early days of the telecommunications data services industry three decades ago to permit competitive forces, not government regulation, to drive the success of that industry. As discussed in greater detail below, the success of the Internet today is, in part, a direct result of those policies. ... First, the Commission noted that data processing services required common carrier facilities and services as necessary inputs, and common carriers that offered their own data services would have the ability and incentive to discriminate against unaffiliated data service providers by denying them access to fairly priced telecommunications services. Second, the Commission noted that common carriers might improperly cross-subsidize their unregulated data processing services with rate-regulated common carrier revenues.

Net Neutrality is perceived as needed today only because the Commission decided to abandon the prior Open Access rules that had been in place for almost 40 years and had served as the foundation upon which the open Internet was able to grow into a primary communications tool. This decision to eliminate Open Access created the underlying problems the Commission now seeks to fix because it produced monopoly or duopoly control over transmission.

3. Congress adopted, applied and extended Open Access in the 1996 amendments.

Congress adopted and reaffirmed the *Computer Inquiry* service unbundling model in the 1996 amendments, and then further extended it through the interconnection and facility unbundling requirements in §§ 251 and 252. But soon after 1996, the Commission abandoned the Open Access policies it had established by serially closing the network, despite Congress's clear policy supporting Open Access.

The 1996 amendments adopted and reaffirmed *Computer Inquiry* in several ways. First, the definitions in § 153 employed the Open Access model by distinguishing between telecommunications services offered by carriers and information services offered by non-carriers. The former retained Title II common carrier obligations, but the latter received virtually no regulation. Congress maintained Open Access by preserving existing "information access" obligations in § 251(g), as well as the right to attach end-user equipment that has been properly registered. Section 257(a) required the Commission to identify and remove entry barriers facing information service providers, and also addressed "provision of parts or services to providers of ... information services." Second, Bell Operating Companies' pathways for entry into the information service market (interLATA information services, electronic publishing and alarm monitoring), which were still denied them at the time, employed both structural separation and

accounting safeguards quite similar to those arising from *Computer II* and *Computer III*, including nondiscriminatory access by unaffiliated information service providers.⁴⁹

Congress used a modified *Computer Inquiry* Open Access framework to require “interconnection” and “facility unbundling” as a means for competitive carriers to enter and participate in the market. The entirety of Sections 251 and 252 is modeled after *Computer Inquiry* Open Access concepts. Section 251(a) and (c)(2) require interconnection between ILECs and competing carriers. Section 251(c)(3) grants competitive carrier access to underlying facilities and infrastructure through facilities unbundling. Nothing in those provisions provides even a hint that broadband was to be excluded, or that use of a different protocol would remove anything from coverage. Instead, Section 251(h)(2) allows the Commission to bring cable companies within the regime.

Enhanced/information service providers formed a significant part of the customer base for the CLEC industry. Past Commissions allowed the incumbents to undercut this relationship in a host of ways and seize the Internet access market all for themselves. That is why we are where we are today.

4. The Commission serially closed the Open Access network between 1999 and 2007.

The Commission decision to abandon Open Access is often said to stem from the *Cable Modem Declaratory Ruling*.⁵⁰ But it actually started before then. Since 1999, the Commission

⁴⁹ See 47 U.S.C. §§ 272(C)(2), 274(d), 275(d), and 276(b)(1)(C) (referencing *Computer III* “nonstructural safeguards” and adopting approach for payphone).

⁵⁰ *Inquiry Concerning High-Speed Access to the Internet Over Cable & Other Facilities; Internet Over Cable Declaratory Ruling; Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities, Declaratory Ruling and Notice of Proposed Rulemaking*, 17 FCC Rcd 4798 (2002) (*Cable Modem Declaratory Ruling*), *aff’d sub nom. Nat’l Cable & Telecomms. Ass’n v. Brand X Internet Servs.*, 545 U.S. 967 (2005).

has consistently declined requests to mandate cable Open Access as a merger condition.⁵¹ The only time that the Commission imposed any access requirements was during AOL's acquisition of Time Warner, however this was done at the insistence of the FTC⁵² and the Commission has not fully enforced the condition.⁵³

In 2002, before the *Cable Modem Declaratory Ruling*, the Commission tentatively concluded that DSL and other broadband services provided by LECs constituted "information services" not subject to Title II tariffing and common carriage requirements. The Commission sought comment on whether it should modify or eliminate *Computer Inquiry* Open Access.⁵⁴ DSL offered by SBC's Advanced Services subsidiary was detariffed the same year.⁵⁵ Then in 2005, the Commission removed all remaining *Computer Inquiry* obligations when it deemed DSL to be an information service.⁵⁶

⁵¹ See *Applications for Consent to the Assignment and/or Transfer of Control of Licenses: Adelphia Communications Corporation (and subsidiaries, debtors-in-possession), Assignors, to Time Warner Cable Inc. (subsidiaries), Assignees et al.*, Memorandum Opinion and Order, 21 FCC Rcd 8203, 8296-99, ¶¶ 217-223 (2006); *Applications for Consent to Transfer of Control of Licenses from Comcast Corp. and AT&T Corp., Transferors, to AT&T Comcast Corp.*, Memorandum Opinion and Order, 17 FCC Rcd 23246, 23299-301, ¶¶ 135-137 (2002); *Applications for Consent to Transfer of Control of Licenses and Section 214 Authorizations from MediaOne Group, Inc., Transferor, to AT&T Corp., Transferee*, Memorandum Opinion and Order, 15 FCC Rcd 9816, 9872-73 ¶ 127 (2000); *Applications for Consent to Transfer of Control of Licenses and Section 214 Authorizations from Tele-Communications, Inc., Transferor, to AT&T Corp., Transferee*, Memorandum Opinion and Order, 14 FCC Rcd 3160, 3205-08, ¶¶ 92-96 (1999).

⁵² See *Applications for Consent to Transfer of Control of Licenses and Section 214 Authorizations by Time Warner, Inc. and America Online, Inc., Transferors, to AOL Time Warner Inc., Transferee*, Memorandum Opinion and Order, 16 FCC Rcd 6547, 6568-69 ¶¶ 57-58 (2001); *America Online, Inc.*, No. C-3989, slip op. at 2, 6-9, 11-17 (F.T.C. Dec. 18, 2000) (Decision and Order), at <http://www.ftc.gov/os/2000/12/aoldando.pdf>.

⁵³ See *In the Matter of Texas Networking, Inc., Petitioner; Petition for Declaratory Ruling and Complaint*, 16 FCC Rcd 17898 (Media Bureau, 2001), Order Dismissing Application for Review, 23 FCC Rcd 6096 (2008).

⁵⁴ *Appropriate Framework for Broadband Access to the Internet over Wireline Facilities*, Notice of Proposed Rulemaking, 17 FCC Rcd 3019, 3029-33 and 3040-43, ¶¶ 17-24 and 43-53 (2002) ("Wireline Broadband NPRM").

⁵⁵ *Review of Regulatory Requirements for Incumbent LEC Broadband Services*, Memorandum Opinion and Order, 17 FCC Rcd 27000 (2002).

⁵⁶ *Wireline Broadband Report and Order*, 20 FCC Rcd 14853, 14860-61 ¶ 9 & n.15, 14862-65, ¶¶ 12-17, 14875-79, ¶ 41-46 & n.107, 14882-98, ¶¶ 32-85, 14904, ¶ 96 (2005) petition for review denied *sub nom. Time Warner Telecom, Inc. v. FCC*, 507 F.3d 205 (3d Cir. 2007).

During this time, the Commission was not content to just allow the incumbents to avoid Open Access for broadband; the Commission also eliminated the §§ 251(c)(4) and 252(d)(3) resale arrangements for independent ISPs⁵⁷ and overlooked serious reports of rules violations raised by independent ISPs.⁵⁸ The Commission also declined Open Access requests when evaluating major telecommunications mergers between SBC and AT&T, Verizon and MCI, and AT&T and BellSouth.⁵⁹

The result of these policy decisions was that the folks that brought the Internet to the masses – independent ISPs – went out of business. Commissioner Copps persistently pointed out this very problem.⁶⁰ The current Commission cannot fairly be held responsible for these

⁵⁷ The *Advanced Services Second Report and Order* applied the resale discount to DSL services offered to end users, but held it did not apply to DSL arrangements made with independent ISPs. *In the Matters of Deployment of Wireline Services Offering Advanced Telecommunications Capability*, Second Report and Order, 14 FCC Rcd 19237, 19247, ¶ 21 (1999), *pet. for review denied sub nom Ass'n of Commc'ns Enters. v. FCC*, 253 F.3d 29 (D.C. Cir. 2001).

⁵⁸ See Texas Internet Service Providers Reply Comments, Docket 00-4 (February 22, 2000), available at <http://apps.fcc.gov/ecfs/document/view?id=6010955248>; Texas Internet Service Providers Reply Comments, Dockets 95-20 and 98-10 (April 30, 2001), available at <http://apps.fcc.gov/ecfs/document/view?id=6512566340>.

⁵⁹ *AT&T Inc. and BellSouth Corp. Application for Transfer of Control*, Memorandum Opinion and Order, 22 FCC Rcd 5662, 5727-31 ¶¶ 116-120, 5742-46 ¶¶ 151-153 (2007); *Verizon Communications, Inc. and MCI, Inc. Applications for Approval of Transfer of Control*, Memorandum Opinion and Order, 20 FCC Rcd 18433, 18507-09 ¶¶ 139-142 (2005); *SBC Communications, Inc. and AT&T Corp. Applications for Approval of Transfer of Control*, Memorandum Opinion and Order, 20 FCC Rcd 18290, 18365-68 ¶¶ 140-143 (2005).

⁶⁰ For example, Commissioner Copps' dissent to the *Broadband 271 Forbearance Order* (19 FCC Rcd at 21517-21519) has proven prescient:

The mismatch between the Commission's broadband rhetoric and reality reaches new heights with today's decision. ... While the country experiences broadband freefall, the Commission has embarked on a policy of closing off competitive access to last mile bottleneck facilities. ... Today, the majority pounds another nail into the coffin it is building for competition. ... [T]here is now absolutely no obligation to provide competitive access to any broadband facilities—from fiber-to-the-home to fiber-to-the curb to packetized functions of hybrid loops to packetized switching capabilities—at just and reasonable rates. [The majority] conclude[s] that the public interest is served by retreating to a policy of non-competition and last mile monopoly control. I cannot support such conclusions nor the underlying analysis.

...

One problem here is that the majority gets so carried away with its vision of the country's telecom future that they act like it is already here, that competition is everywhere flourishing, and that intermodal competition is already ubiquitous reality. But their cheerful blindness to stubborn market reality actually pushes farther into the future the kind of competitive telecom world they say they want.

...

policy decisions, but it can and should undo the damage by reinstating Open Access and reinvigorating competition for Internet access.

5. The Commission also eliminated UNE-based Open Access.

The Commission at first made significant, but incomplete efforts to apply Open Access principles to UNEs. The *Local Competition Order* declined to subject packet switches to UNE access requirements and ruled that collocation did not extend to equipment used to provide enhanced services. The Commission did allow multifunction equipment supporting both conventional telephone and enhanced services so long as that equipment was necessary to providing conventional telephone service. The Commission also held that any company obtaining interconnection or UNE access to provide telecommunications services could offer information services through the same arrangement. The order mandated UNE access to all loops connecting central offices to end users, including the loops used to provide DSL and obligated incumbent local telephone company to fulfill any requests to condition existing loops to make them DSL-compatible.⁶¹ A subsequent order confirmed that collocation included multifunction equipment that could be used to provide both voice and data services.⁶² Perhaps most importantly, the *Line Sharing Order* mandated UNE access to the high frequency portion of the loop used to carry DSL so that two competitors could provide services over the same loop,

The lack of analysis in this proceeding—and in the Commission’s approach to broadband generally – amounts to a regulatory policy of crossing our fingers and hoping competition will somehow magically burst forth. ... if we want to enter the brave new world of broadband, we need to move away from our current course. The facts show we are headed in the wrong direction at warp speed. I dissent.

⁶¹ *Implementation of the Local Competition Provisions in the Telecommunications Act of 1996*, First Report and Order, 11 FCC Rcd 15499, 15691-92, 15713, 15794-95, and 15990, ¶¶ 380-382, 427, 580-581, and 995 (1996).

⁶² *Deployment of Wireline Services Offering Advanced Telecommunications Capability*, First Report and Order and Notice of Proposed Rulemaking, 14 FCC Rcd 4761, 4776-79, ¶¶ 27-31 (1999).

with one offering conventional telephone service in the lower frequencies and the other offering DSL in the upper frequencies.⁶³

The courts were admittedly no great help to Open Access. The Supreme Court's decision in *AT&T Corp. v. Iowa Utilities Board* remanded the Commission's initial UNE access rules because the Supreme Court held the Commission had construed the "necessary" and "impair" standards too broadly.⁶⁴ On remand, the Commission reiterated that incumbent local telephone companies must condition DSL loops upon request. Although UNE access to loops generally included all attached electronics, the Commission nonetheless again specifically excepted packet switches and DSLAMs, based on the notion that granting UNE access to them would deter investment in a nascent market. The Commission did permit UNE access to DSLAMs located in remote terminals that were too small to permit physical collocation, but to date this "right" was rarely actualized into viable and functional CLEC arrangements – largely because of ILEC roadblocks.⁶⁵

In 2000, the D.C. Circuit struck down the Commission's decision permitting the collocation of multifunction equipment.⁶⁶ In response, the Commission revised its rules in 2001 to limit collocation of multifunction equipment to equipment whose primary purpose is to provide the requesting carrier either with interconnection that is "equal in quality" to that provided by the incumbent local telephone company for its own services or with

⁶³ *Deployment of Wireline Services Offering Advanced Telecommunications Capability*, Third Report and Order and Fourth Report and Order, 14 FCC Rcd 20912 (2000).

⁶⁴ *AT&T Corp. v. Iowa Utils. Bd.*, 525 U.S. 366, 387-92 (1999).

⁶⁵ *Implementation of Local Competition Provisions of Telecommunications Act of 1996*, Third Report and Order and Fourth Further Notice of Proposed Rulemaking, 15 FCC Rcd 3696, 3775, 3776-77, 3783-84, 3835-37, 3839-840, ¶¶ 172, 175, 190-194, 306-309, 314-317 (1999).

⁶⁶ *GTE Serv. Corp. v. FCC*, 205 F.3d 416, 422-24 (D.C. Cir. 2000) (quoting 47 U.S.C. § 251(c)(6)).

“nondiscriminatory access” to an unbundled network element.⁶⁷ These revisions to the collocation rules survived review in the face of challenges from ILECs.⁶⁸

The Commission then began a broader retreat from any real effort to extend the regulatory regime applicable to conventional telephone service to DSL and other wireline broadband technologies. In 2002, the Commission issued the *Wireline Broadband NPRM*, which tentatively concluded that DSL and other broadband services provided by local telephone companies constituted “information services” not subject to Title II tariffing and common carriage requirements, and sought comment on whether to modify or eliminate *Computer Inquiry* rules.⁶⁹ Later in 2002, the Commission detariffed DSL services that SBC offered through its separate subsidiary.⁷⁰

In 2002, the D.C. Circuit struck the Commission’s decision requiring line sharing.⁷¹ This led the Commission to eliminate line sharing and lift UNE access obligations to most high-capacity loops in the 2003 *Triennial Review Order*. The Commission also eliminated the limited exceptions it had recognized for UNE access to DSLAMs and other packet switching equipment.⁷² The *Triennial Remand Review Order* then eliminated high-capacity transport and

⁶⁷ *Deployment of Wireline Services Offering Advanced Telecommunications Capability*, Fourth Report and Order, 16 FCC Rcd 15435, 15452-60, ¶¶ 32-44 (2001).

⁶⁸ *Verizon Tel. Cos. v. FCC*, 292 F.3d 903 (D.C. Cir. 2002).

⁶⁹ *Appropriate Framework for Broadband Access to the Internet over Wireline Facilities*, Notice of Proposed Rulemaking, 17 FCC Rcd 3019, 3029-33 ¶¶ 17-24, 3040-43 ¶¶ 43-53 (2002).

⁷⁰ *Review of Regulatory Requirements for Incumbent LEC Broadband Services*, Memorandum Opinion and Order, 17 FCC Rcd 27000 (2002).

⁷¹ *United States Telecom Ass’n v. FCC*, 290 F.3d 415, 428-29 (D.C. Cir. 2002).

⁷² *Review of the Section 251 Unbundling Obligations of Incumbent Local Exchange Carriers*, Report and Order and Order on Remand and Further Notice of Proposed Rulemaking, 18 FCC Rcd 16978, 17327-33 ¶¶ 549-580 (2003).

high-capacity loops from the list of § 251(c)(3) UNEs.⁷³ The Commission granted forbearance from 271 requirements for broadband in 2004.⁷⁴

In sum, the situation today is that an independent ISP has no means to obtain high-capacity loops from an ILEC or a cable company under nondiscriminatory and reasonable terms, either directly or through a competitive carrier. There is no wholesale access to network infrastructure or services provided on fair and reasonable terms, for which there is some degree of transparency and non-discrimination. There is no mandatory regulated access, such as local loop unbundling, and other wholesale access products such as dark fiber or next layer (e.g., bitstream) are unavailable, except by leave and on adhesive “negotiated” terms reluctantly offered by a cable or telephone company.

Open Access is gone, and with it, the independent ISP industry that originally brought the Internet to the masses. The fact is the Commission’s predecessors made a series of decisions that led to the elimination of a source of robust competition and beneficial economic incentives. This history, however, need not dictate future policy choices. This Commission now has the opportunity to change course and bring Open Access and competition back to American broadband.

⁷³ *In re Unbundled Access to Network Elements Review of the Section 251 Unbundling Obligations of Incumbent Local Exchange Carriers*, 20 FCC Rcd. 2533, 2575-641 (2005), *aff’d*, *Covad Commc’ns Co. v. FCC*, 450 F.3d 528 (D.C. Cir. 2006).

⁷⁴ *Petition for Forbearance of the Verizon Telephone Companies Pursuant to 47 U.S.C. § 160(c)*; *SBC Communications Inc.’s Petition for Forbearance Under 47 U.S.C. § 160(c)*; *Qwest Communications International Inc. Petition for Forbearance Under 47 U.S.C. § 160(c)*; *BellSouth Telecommunications, Inc. Petition for Forbearance Under 47 U.S.C. § 160(c)*, Memorandum Opinion and Order, 19 FCC Rcd 21496 (2004) (*Broadband 271 Forbearance Order*).

6. Commission predictions that closing the networks would lead to ubiquitous broadband and not threaten the open Internet have proven incorrect.

When the Commission classified cable broadband Internet access and DSL Internet access as information services, it predicted that broadband competition would take off as a result. The *DSL Reclassification Order* explained that deregulation was appropriate because competition amongst independent ISPs was flourishing and would continue to thrive.⁷⁵ The Commission also believed that intermodal competition would blossom, leading to additional investment and reduced prices for consumers.⁷⁶ This expectation was not merely peripheral to the decision to classify broadband as an information service, it was the primary basis for Title I classification.⁷⁷ Yet nearly a decade since the *Cable Modem Declaratory Ruling* was issued, at a time when the Commission expected broadband competition to be in full bloom, the current *NPRM* instead acknowledges that Americans have “limited choice between broadband providers in many areas of the country.”⁷⁸

Not only did these expectations fail to materialize, but the classification decisions based upon these expectations have proven counterproductive. The competition that existed at the time of the orders has vanished. In 1998, there were between five thousand and seven thousand independent ISPs offering Internet access to the American public,⁷⁹ but today almost all of them are gone. The independent ISPs are the collateral damage of the Commission’s misjudgment that, in a deregulatory environment, “wireline platform providers will find it necessary and

⁷⁵ *Appropriate Framework for Broadband Access to the Internet Over Wireline Facilities*, 20 FCC Rcd 14853, 14907, ¶ 100 (2005) (*DSL Reclassification Order*).

⁷⁶ *Id.*, ¶ 57.

⁷⁷ *Id.*, ¶ 44.

⁷⁸ *NPRM* at ¶ 48.

⁷⁹ Barbara Esbin, *Internet over Cable: Defining the Future in Terms of the Past* 18 & n.88 (Fed. Commc’n Comm’n Office of Plans and Policy, Working Paper No. 30, 1998).

desirable to negotiate arrangements with unaffiliated ISPs for access to their broadband networks in order to grow the base of users of their broadband infrastructures.”⁸⁰ The Commission predicted that deregulation would ensure these ISPs “continued availability of this transmission component, under reasonable rates, terms, and conditions.”⁸¹ Instead, the incumbent telephone and cable companies closed their networks and began offering broadband Internet access on monopoly terms.

All of the problems that the *NPRM* attempts to remedy arise from an uncompetitive broadband market. If American Internet users had the option to vote with their feet, the marketplace would punish harmful behavior. Users themselves could impose neutrality requirements by ditching broadband providers with abusive practices. A Comcast decision to inject reset headers into its users’ BitTorrent traffic would be weighed against the loss of customers and shareholder fury, rather than the merits of challenging the Commission’s Section 706 authority in court.

Not only did the Commission miss the mark on its prediction that intramodal competition would thrive, but it also misjudged the likelihood of intermodal competition. The *DSL Reclassification Order* argued that “other existing and developing platforms, such as satellite and wireless, and even broadband over power line in certain locations, indicat[e] that broadband Internet access services in the future will not be limited to cable modem and DSL service.”⁸² However, none of these technologies have developed into a competitive threat to the telephone and cable companies. Wireless broadband has developed its own niche, but has failed to become an alternative for wired Internet access because of limitations inherent to broadcasting data over

⁸⁰ *DSL Reclassification Order*, 20 FCC Rcd 14853, 14895 ¶ 79.

⁸¹ *Id.* at ¶ 100.

⁸² *Id.* at ¶ 50.

radio spectrum. Eighty-three percent of smartphone owners continue to maintain their wired home broadband connections, indicating that wireless is not a viable replacement.⁸³ If the average American Internet user were to even attempt to substitute a wireless connection for their wired connection, overage charges would drive their bill to more than \$800 per month.⁸⁴ Indeed, the fact that the *NPRM* proposes to allow non-neutral wireless broadband service shows that it is not yet a fully substitutable and competitive equivalent for wired service.

In addition to unrealistic expectations regarding competition, the Commission also incorrectly predicted that infrastructure investment would take off. The telephone and cable companies assured the Commission that they would make commercially-reasonable alternative facilities available to unaffiliated ISPs.⁸⁵ The Commission believed them and agreed that ending Open Access was an acceptable concession for the promised broadband deployment. However, the promised investment has not occurred.

The incumbents robustly improved the telecommunications network for decades even after Open Access principles were first developed in the 1960s. The Commission embraced Open Access as a means to facilitate competition in a series of cases related to interconnection, customer premises equipment, inside wiring and enhanced/information services. The incumbents had no real choice but to continue investing, because their profits came from a return on investment under traditional regulatory principles; if they failed to make new investment they earned less profit.

In hindsight, the fact that competition didn't develop in an unregulated environment should not come as a surprise. From a practical perspective, companies that sell wires will only

⁸³ Susan P. Crawford, *First Amendment Common Sense*, 127 Harv. L. Rev. 2343, 2355-56 (2014).

⁸⁴ *Id.*

⁸⁵ See, e.g., *DSL Reclassification Order* 20 FCC Rcd 14853, 14886-87 ¶¶ 63-64; see also *Broadband 271 Forbearance Order*, 19 FCC Rcd at 21508, ¶ 26.

survive in a competitive market if they assiduously tend to making new wire. On the other hand, if that company faces little competition in the wire market, it can earn extraordinary profit from both wire and adjacent products that use wires by restricting output and keeping the price high. The rest of the developed world understands this incentive and has maintained Open Access. Some commentators have observed that domestic capital investment and employment growth have slowed since the mid-2000s, while overseas investment – even under Open Access – has accelerated, especially when analyzed on a constant-dollar basis⁸⁶ AT&T and Verizon have reduced or ended their network extension efforts and essentially yielded to the cable companies in many areas.

The problem does not reside with those who provide Internet; it arises because transmission is still a monopoly (or a duopoly). From a technical and economic perspective, transmission and Internet access are two separate markets, although they are adjacent.⁸⁷ Once again, the Commission recognized this very fact in the *Computer Inquiries*. The very purpose of that proceeding was to isolate monopoly components and impose regulation on monopoly activity, while deregulating potentially competitive enhanced services.

The broadband service sector could become fully competitive again if the underlying bottleneck transmission components are available on a common carrier basis to all potential purchasers. That is precisely how it worked in the dial-up days and the move to broadband does not justify a different result. If we return to Open Access and allow competition back into the

⁸⁶ See, e.g., S. Derek Turner, Fighting the Zombie Lies: Sorry ISPs, Title II Is Good for the Economy, TM + © 2009–2014 Free Press, available at <http://www.freepress.net/blog/2014/05/14/fighting-zombie-lies-sorry-isps-title-ii-good-economy> (“Investment: Under Title II, Bell Company capital investments increased by 20 percent (a CAGR of 1.8 percent). But after the Commission removed Title II, capital investment at these companies declined by 5 percent (a CAGR of negative 0.7 percent). ... Jobs: Bell Company jobs are down 20 percent since the removal of Title II. Employment at these companies peaked in 2000 following the period when the Bells were subjected to the most comprehensive implementation of Title II.”).

⁸⁷ Internet Access depends on transmission service inputs, but they are logically and practically separate markets. From an antitrust perspective, the Commission basically allowed the incumbents to engage in monopoly leveraging and then a tying arrangement.

Internet access market, then any Internet access provider that fails to act consistent with consumer expectations will quickly be faced with alternative providers offering prices and terms that users really want.⁸⁸ As it stands, however, the last mile transmission input is available only to the telephone and cable companies for Internet access. They therefore can now monopolize both the transmission and the Internet access. The Commission had recognized for 40 years that this kind of vertical integration and leveraging inexorably leads to discrimination and rationing as a means to keep prices and profits artificially high. But the rules put in place to prevent these predictable harms were jettisoned in favor of still-unfulfilled investment promises and expectations that competition would thrive.

V. TITLE II RECLASSIFICATION WOULD BE BASED ON THE COMMISSION’S WELL-ESTABLISHED LEGAL AUTHORITY AND WOULD NOT BE SUBJECT TO REJECTION BY THE COURTS.

The Commission’s decision to classify cable modem service as an information service was affirmed in *Brand X*, largely due to *Chevron* deference. A decision to reclassify the transmission component of broadband Internet access – or broadband Internet access itself – would again receive *Chevron* deference from the courts. The decision could be well-reasoned and supportable because broadband providers clearly constitute common law common carriers. But there are lessons to be learned by reviewing the premises and expectations upon which the classification decision was based.

First, it is noteworthy that the *Cable Modem Declaratory Ruling* glossed over the fact that many if not most cable companies have historically provided “telecommunications service”

⁸⁸ Many of the activities identified as “problems” in this entire debate would not much of a concern if there was a competitive market. A provider’s attempt to impose “content value” pricing, or even “discrimination” simply would not succeed if there were alternatives – unless consumers decided that is what they actually want. If that is what they want, then the activity is merely fulfilling consumer desires and that is a good thing. The problem arises when the two dominant providers impose these results, *despite* rather than *because of* consumer desires.

(“basic service” under *Computer Inquiry I*), albeit perhaps not for “broadband Internet access.”⁸⁹ Several were, in fact, common carriers. Several also offered “telecommunications” on a private carrier basis, including a few that successfully convinced the Commission to preempt state efforts to impose intrastate common carrier regulation over their “telecommunications” offering.⁹⁰

Cox/CoxDTS and *United Cable* centered on state commission efforts to regulate cable company institutional high-speed digital transmission services. The “high-speed digital transmission service” supported *enhanced services* supplied by “governmental and educational institutions and private businesses.”⁹¹ Presumably *United Cable*’s high-speed digital transmission service was or could also be used to support enhanced operations as well.

This was “telecommunications.” This was “broadband.” It was used (at least in part) to support enhanced functionalities. In *Cox/Cox DTS* the Commission chose to not impose common carriage on Comcline’s service. Cox’s “DTS” service, however, was common carrier although it enjoyed “forbearance” from tariffing.⁹² These cases demonstrate that cable companies have provided broadband transmission “telecommunications,” some of which was a “telecommunications service,” and this transmission product was used to support enhanced/information services supplied by unaffiliated private and public third parties. The case was about “broadband data services.”⁹³ The *Cable Modem Declaratory Ruling* overstated one of its premises by overlooking the fact that cable companies had indeed offered a stand-alone

⁸⁹ See *Cable Modem Declaratory Ruling*, 17 FCC Rcd at 4824-4826, 4828, ¶¶ 42-46, 51.

⁹⁰ See e.g., *In the Matter of Cox Cable Communications, Inc., Comcline, Inc. and Cox DTS, Inc.*, Declaratory Ruling, and Order, 102 F.C.C.2d 110, 120-21 ¶¶ 24-25 (1985), vacated as moot on other grounds, 1 FCC Rcd 561 (1986); see also *In the Matter of United Cable Television of Colorado, Inc., et al*, Memorandum Opinion and Order, 1 FCC Rcd 555 (1986) (recognizing the cable company service is telecommunications, but refusing to preempt).

⁹¹ See *Cox*, 102 F.C.C.2d 110, 112 ¶ 3.

⁹² *Id* at 128, ¶ 36, citing to *Competitive Carrier Rulemaking*, Fifth Report and Order, 98 FCC 2d 1191, 1205-09 (1984).

⁹³ *Id* at 132 (Quello, dissenting).

broadband transmission service, and several of those were offered on a common carrier basis. Further, some of those were used to support enhanced services provided by the subscriber to the service.

Further, few seem to recall that *NARUC II* involved two-way non-video cable company provided transmission service offerings that were ultimately held by the court to be common carrier. The Commission had preempted state regulation and refrained from imposing common carriage. The *NARUC II* court reversed, however, and held that the specific offer in issue there was telecommunications and should have been treated as common carrier because it met all the relevant indicia of common carriage.⁹⁴ “The clear content of that term (common carrier) as developed at common law and discussed in our previous *N.A.R.U.C.* opinion indicates that most or all of the two-way, non-video cable operations at issue here do fit within the common carrier concept. Because at least the bulk of those activities are also clearly intrastate, we cannot avoid the conclusion that the § 152(b) jurisdictional bar clearly applies, beyond any margin for deference or discretion.”⁹⁵

All seem to agree that cable companies’ broadband transmission is telecommunications and both the Commission and courts have recognized that some of their offerings can be, or are, common carrier and thus telecommunications service. The question then becomes whether the Commission should – after the experience gained over the last several years – decide that it will isolate the transmission portion in issue today and require that it be offered on a common carrier basis going forward, by declaring that the transmission involved here is and should be a “telecommunications service.” The answer to both parts of this question should be “yes.”

⁹⁴ *NARUC II*, 533 F.2d at 608-610.

⁹⁵ *Id* at 618.

Although the Commission decided not to impose or find common carriage in the *Cable Modem Declaratory Ruling*, the cable companies' current offerings of bundled Internet access most certainly do meet the holding out and indifference prongs. They have a standard offer and do not negotiate individual contracts, particularly for residential and small-business customers. They typically hold out to serve all comers that meet their eligibility criteria. They do not generally choose clients on an individual basis or determine in each particular case whether and on what terms to serve.⁹⁶ They meet all of the indicia of common carriage under the common law. While the Commission has not required common carriage, the cable companies have exhibited all the classic signs of a voluntary undertaking to be a common carrier.

It is true that *NARUC I*⁹⁷ states that the Commission does not have “unfettered discretion” to “confer or not confer common carrier status on a given entity, depending upon the regulatory goals it seeks to achieve” and went on to hold that “[t]he common law definition of common carrier is sufficiently definite as not to admit of agency discretion in the classification of operating communications entities. A particular system is a common carrier by virtue of its functions, rather than because it is declared to be so.”⁹⁸ However, if an entity or class of entities has voluntarily chosen to act like a common carrier, then the Commission can and should recognize that reality, and proceed accordingly. “If practice and experience show the [cable companies and telephone companies] to be common carriers, then the Commission must determine its responsibilities from the language of the Title II common carrier provisions.”⁹⁹ The actual operations of cable and telephone companies' broadband Internet access services

⁹⁶ Cf. *NARUC II*, 533 F.2d at 608-09; *NARUC I*, 525 F.2d at 643; see also *Southwestern Bell Tel. Co. v. FCC*, 19 F.3d 1475, 1481 (D.C. Cir. 1994).

⁹⁷ *NARUC I* involved whether the Commission could deem a particular wireless service to not be common carrier and pre-empt state regulation.

⁹⁸ *NARUC I*, 525 F.2d at 644.

⁹⁹ *Id.*

“appear(s) to bring them within the common carrier definition.”¹⁰⁰ Experience has shown that there are “reasons implicit in the nature of [broadband Internet access] operations to expect an indifferent holding out to the eligible user public.”¹⁰¹ The cable and telephone companies’ actual manner of providing retail Internet access services easily meet the *NARUC* common carrier tests. Title II can and should be applied. Then the Commission should require unbundling of the transmission component.

The Commission has the power to require unbundling and a stand-alone common carrier offer. The *NARUC I* court expressly contemplated this result by asking whether “there will be any legal compulsion thus to serve indifferently.”¹⁰² The court recognized that as a valid question and engaged in an analysis of whether there was (and thus could be) a compulsion, so there is room for regulators to compel common carrier classification in appropriate circumstances, especially when the providers are already acting consistent with that designation in their actual dealings.

i2Coalition believes that the proper choice is to return to Open Access by using Title II authority and mandating unbundling of the transmission component. If this is done, the Commission does not need to regulate Internet access because competition will sufficiently constrain the dominant actors. If, however, the Commission does not return to Open Access, then it *is* necessary to regulate broadband Internet access under Title II because the dominant providers face no competitive constraints. If the Commission is going to eliminate the Internet access evils identified in the *NPRM* through direct regulation, then effective and clear prohibitions on blocking and unreasonable discrimination are imperative. Since that is *per se*

¹⁰⁰ *Id.*

¹⁰¹ *Id.* at 643.

¹⁰² *Id.*

common carriage, the Commission should invoke its common carrier jurisdiction and use Title II tools.

VI. MOBILE AND FIXED BROADBAND SERVICE SHOULD BE SUBJECT TO EQUAL AND CONSISTENT RULES.

The *NPRM* proposes to maintain the *Open Internet Order*'s mobile no-blocking rule, and thus maintain inconsistent requirements for fixed and mobile broadband. i2Coalition supports the principle of technology neutral rules and believes that the same no-blocking rule should be applied in a consistent manner. Separate rules and standards entrench differences, rather than encourage convergence and competition. If wireless broadband is ever to become a viable alternative to wired broadband, the product should not evolve with different regulatory expectations that become more ingrained and permanent over time.

Of note, the current and proposed rule for mobile broadband is also far less robust than the standards imposed for Upper 700 MHz C-Block mobile licensees. For example, Verizon's previous blocking of tethering that led to the settlement described in *NPRM* at paragraph 41 and note 93 would not be a violation of the current and proposed mobile no-blocking rule, since it does not at all address attachment of devices and speaks only to "applications that compete with the provider's voice or video telephony services."¹⁰³ The *NPRM* cites other examples of mobile blocking that were mentioned in *Open Internet Order*.¹⁰⁴ The current and proposed mobile no-blocking rule would likely prohibit the blocking of Skype, because it at least arguably competes with voice service. However, it would not ban blocking many alternative online payment services since they are not always provided via a website (and often involve installing an

¹⁰³ The proposed mobile no-blocking rule would probably outlaw AT&T's prior actions blocking FaceTime that is also referenced in *NPRM* at paragraph 41.

¹⁰⁴ *NPRM* at ¶ 53.

application)¹⁰⁵ and are not voice or video telephony services. Similarly, the rule would not ban a mobile provider from blocking Slingbox¹⁰⁶ or peer-to-peer applications. The *Open Internet Order* decided to have a “targeted prophylactic rule” restricting “only practices that appear to have an element of anticompetitive intent” and held that restrictions regarding applications that compete with a mobile providers’ voice or video telephony offerings was “appropriate at this time” in lieu of a “broader no-blocking rule.”¹⁰⁷ The Commission said it would “monitor” developments and reassess should the need arise.¹⁰⁸

The Commission should indeed revisit its original decision and apply the same no-blocking rules to both fixed and mobile broadband service.¹⁰⁹ Consistency is a far superior policy. Any technical differences based on network technology that may justify a different outcome can be dealt with through the “subject to reasonable network management” exception.

VII. CASE STUDY: PRIVACY AND ENCRYPTION

A. Paid prioritization arrangements are a threat to Internet privacy.

The *NPRM* gives significant consideration to content-based network practices, but never stops to consider the privacy implications for American Internet users. The Commission discusses at great lengths whether paid priority arrangements are consistent with an open Internet and if they could be implemented on a commercially reasonable basis, yet never seems to realize that it is contemplating the wholesale monitoring of the content of Americans’ broadband Internet connections.

¹⁰⁵ Cf. *Open Internet Order*, 25 FCC Rcd at 17960 ¶ 100.

¹⁰⁶ Slingbox may or may not be a “video service” depending on how that is defined, but it is clearly not a “video telephony service” and therefore would be excluded from protection.

¹⁰⁷ *Open Internet Order*, 25 FCC Rcd at 17961 ¶ 101.

¹⁰⁸ *Id.* at 17962 ¶¶ 104-105.

¹⁰⁹ *NPRM* at ¶ 62.

However, any arrangement in which a broadband ISP provides priority treatment to an edge provider necessarily contemplates content monitoring. For example, should Comcast enter into paid prioritization deal with Netflix, Comcast will need technological means to identify the Netflix traffic subject to the arrangement. This will require that Comcast, at a minimum, monitor the services, applications, devices, and websites with whom its customers are communicating. Furthermore, Section 8.9 of the proposed rules officially sanctions copyright enforcement efforts by broadband Internet access providers. This would mean that broadband providers now have the blessing of the Commission to open up their end users' packets to filter content. Unless there is a competitive market where users have choices among multiple broadband Internet access providers, the Commission should uphold Americans' privacy rights and be wary of content inspection-based services.

B. The proposed rules fail to account for encryption technologies.

Internet users themselves are quite concerned about the privacy of their online communications. Virtual private network (VPN) services are thriving. Other privacy applications like the TOR browser are becoming increasingly popular. Edge providers are providing privacy enhancing options and the use of SSL encryption has become ubiquitous. It is generally considered a positive development that American Internet users are becoming more jealous of their fundamental privacy rights. The Commission should not adopt policies that frustrate Americans' exercise of their civil liberties and should instead encourage such behavior.

This proliferation of encryption-based privacy tools presents significant uncertainty to the viability of the *NPRM*'s proposed paid priority regime. For example, how could Comcast prioritize Netflix traffic (to use the example above) when an end user utilizes an encrypted VPN service? Would that user have to choose between their privacy and their ability to access Netflix

as intended? Would Comcast have the right to decrypt encrypted traffic in order to make prioritization decisions? Section 8.9 of the proposed rules permits “reasonable” efforts to address unlawful content. Does that include decryption to filter for copyrighted content, or even an outright ban on encryption because it would interfere with efforts to address unlawful content? Would encrypted traffic constitute lawful traffic subject to the no-blocking rule even though encryption is sometimes used to mask unlawful traffic? The no-blocking rule for mobile broadband only prevents the blocking of applications with which the wireless carriers compete. Therefore, can mobile broadband providers block encryption tools that Internet users utilize to protect their online privacy?

The example of encryption and privacy demonstrate that the market does not neatly fit into the Commission’s proposed definitions and rules. Nor do the rules meet users’ desires and needs. A paid priority regime assumes that innovation will only occur at the minimum level of service. It assumes that all Internet traffic is and will remain transparent to broadband access providers. It also ensures that innovation at very high bandwidth levels is only available to existing, successful edge providers with the means to purchase prioritization. Fundamentally, the Commission is attempting to limit the future Internet to the confines of today’s Internet, which favors the current large market participants over small players. Innovation and the market are unpredictable. The best way to ensure that the Internet remains open well into the future is by ensuring that competition exists on all parts of the network, especially the presently-closed last mile transmission component.

VIII. ANALYSIS OF THE TEXT OF THE PROPOSED RULES

i2Coalition offers the following observations and recommendations on the text of the proposed rules.

A. Authority for Part 8 Rules

NPRM Appendix A sets out the proposed rules. The Appendix states that the authority for the rules is derived from 47 U.S.C. §§ 151, 152, 154(i)-(j), 303, 316 and 1302. The Commission should also invoke its Title II authority. As explained above, i2Coalition does not believe the Commission should impose common carrier regulation on “Internet access” at this point and should instead reinstate Open Access so competition can return to the Internet access market. Title II is a necessary prerequisite to reinstating Open Access through *Computer Inquiry* type rules. But if the Commission does choose to regulate Internet access and wants rules that are meaningful and effective to deter the harms identified in the *NPRM*, then Title II is a prerequisite as well. As shown above, the no-blocking and commercially reasonable rules are *per se* common carrier obligations. The Commission should expressly rely on its Title II authority as the basis for these rules because § 706 (47 U.S.C. § 1302) on its own does not provide sufficient authority to promulgate or enforce common carrier rules. Therefore, references to §§ 201, 202, 203, 204, 205, 206, 208, 209, 211, 215, 218, 219, 220, 251 and 252 should be added. Given that it may be appropriate to forbear from applying some of the above-listed statutory provisions, a reference to § 160 should be added as well.

The following analysis and recommendations on the proposed rules assumes a decision to regulate Internet access either in addition to or instead of returning to Open Access.

B. Transparency Rule

The transparency rule should expressly require meaningful and plain-English disclosures of practices and policies that impact user privacy. Specifically, i2Coalition recommends that a new subsection (d) be added to § 8.3 stating as follows:

(d) A person engaged in the provision of broadband Internet access service shall have a publicly-available privacy policy that meaningfully explains what user

information is gathered, how it is gathered, the purposes for which any user information that is gathered will be used, and to whom user information will be disclosed and under what circumstances. The privacy policy must be a part of any contractual relationship with each user and enforceable as such. The privacy policy must state whether the provider employs Deep Packet Inspection and inspects content, and if so for what purpose(s) Deep Packet Inspection is employed, and disclose each purpose for which the information collected or gleaned from collected information is used; the length of time any intercepted content or derived information is stored; and the specific circumstances under which any intercepted content or derived information will be disclosed to third party governmental or private entities. If a provider does employ Deep Packet Inspection and retains any user content or information derived from such content, the privacy policy must expressly provide that the provider does not assert any ownership or property rights to the content or derived information, and all property rights remain with the original owner of the content, e.g., the edge provider or end user.

C. No-Blocking Rule

The simplest way to reinstate a workable no-blocking requirement would be to accept, indeed embrace, the concept that no blocking is a *per se* common carrier obligation, and apply Title II. The Commission should also eliminate the proposed different treatment between fixed and mobile broadband. The Commission should apply one no-blocking standard.

As explained above, the same concerns apply to both fixed and mobile, and the basic rule should be the same. Different treatment will invite gaming the definitions by all sides: those that want the harsher rule to apply will try to argue that the wireless service is fixed, while the wireless provider will say it is mobile.

The lesser standard will allow wireless broadband providers to block content from sources other than lawful websites. The Internet, however, is far more than just a collection of websites and content can be acquired from or sent to Internet destinations that are not on the web. Content is available from and is routinely sent to servers that are not based on HTML. The mobile no-blocking obligation should apply to all content.

The draft mobile wireless no-blocking rule only prohibits providers from blocking “applications that compete with the provider’s voice or video telephony services.” It would therefore allow a mobile provider to block any application that is not voice or video telephony. If the wireless provider does not offer video telephony, then it could block such applications. The rule would allow the wireless provider to block email applications or individual emails. The rule would allow the wireless provider to block the great preponderance of applications and services that presently exist.¹¹⁰ The rule would allow wireless providers to block encryption and virtual private networks, which are useful for privacy-conscious individuals and imperatives for many businesses and their employees.

D. “Commercially reasonable” vs. “No unreasonable discrimination”

The Commission should abandon the pretext of banning unwanted discrimination through the commercially reasonable rule, expressly invoke Title II and then proceed to ban unreasonable discrimination. “Unreasonable discrimination” should be further defined, and broader than the discrimination rule contained in the now-vacated § 8.7. The *Open Internet Order* indicated that use-agnostic differential treatment would not be unreasonable.¹¹¹ The original rule prevented discrimination yielding anti-competitive results, as well as other forms of discrimination not based on anti-competitive intent, but still deemed harmful to the public interest.¹¹² Nonetheless, the Commission indicated that some forms of discrimination based on application, content, services, use, source/destination or device might not be unreasonable. For example, *Open Internet Order* ¶ 71 explained that “packet prioritization” as part of service to consumers is likely

¹¹⁰ If one peruses the app stores for Apple, Google, Microsoft, or any of the others offering mobile apps, it quickly becomes apparent that voice and video telephony apps are a small minority in comparison to other kinds.

¹¹¹ *Open Internet Order*, 25 FCC Rcd at 17946 ¶¶ 73 and 75. Commenters sometimes call for “application-agnostic” rules, but this characterization is actually a shorthand way of describing concerns over differential treatment of applications, content, services, use, source/destination or device based on network provider choices rather than user choice or desire.

¹¹² *Open Internet Order*, 25 FCC Rcd at 17949 ¶ 78.

not unreasonable discrimination. This could be read to allow prioritization regimes regarding specific applications, content, services, use, source/destination or devices determined solely by the network provider and independent of (and perhaps even despite) user desire.

If the Commission decides to continue regulating Internet access, it should invoke Title II and reinstate the “no unreasonable discrimination” rule. It should then make clear that discrimination between or among applications, content, services, use, source/destination or devices determined solely by the network provider and independent of user desire is unreasonable discrimination. The rule should be truly use agnostic – except where *the user* requests differential treatment.

E. Other Laws and Considerations

The Commission proposes to retain § 8.9. i2Coalition believes that the final sentence invites and encourages Internet access providers to invasively surveil user activity, or at least give permission for providers to inspect users’ content. It therefore implicitly blesses invasions of privacy. The entire sentence should be stricken, or clarified in some fashion so it cannot be used as a defense to or justification for content inspection absent express user consent.

F. § 8.11 Definitions

1. Definition of “Block” (8.11(a))

The proposed definition for “block” should not exclusively focus on what is being delivered to the *edge provider* for purposes of assessing whether a “minimum level of access” is not being provided and thus there is blocking. The Commission should be at least equally (if not exclusively) concerned with whether the end user is receiving an adequate level of access that allows the end user to simultaneously send information to and receive information from all desired endpoints, both individually and collectively.

The proposed definition should be amended to reinforce that the purpose of the no-blocking obligation: to ensure that users may send or receive desired content and employ the “applications, services, or non-harmful devices” they choose.

i2Coalition recommends this text for the final definition:

The failure of a broadband Internet access service to provide ~~an edge provider with a minimum level of access~~¹¹³ that is sufficiently robust, fast, and dynamic for effective use by end users and edge providers, and allows end users to send or receive desired content and employ the applications, services, or non-harmful devices they choose.

2. Definition of “Broadband Internet access service” (8.11(b))

The Commission proposes to retain the original definition for Broadband Internet Access Service promulgated in the *Open Internet Order*. i2Coalition believes it should be changed.

The present and proposed definition states as follows:

(a) Broadband Internet Access Service. A mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up¹¹⁴ Internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence, or that is used to evade the protections set forth in this Part.

¹¹³ i2Coalition has significant concerns with the proposal to define a “minimum level of access” in order to then allow priority services to edge providers that exceed that level. The avowed purpose is to have a back-door means to prevent unreasonable discrimination while purporting to satisfy the D.C. Circuit’s reasons for vacating the discrimination rule. i2Coalition believes that – if the Commission decides to regulate Internet access – the Commission should instead proceed to invoke Title II and reinstate the no-discrimination rule under that authority. Thus, we have stricken the reference to minimum level of access in this proposed edit is made in the alternative. If the Commission persists in taking the approach proposed in the *NPRM* then the reference to “minimum level of access” should be retained.

¹¹⁴ *Open Internet Order*, 25 FCC Rcd at 17935 ¶ 51. The Commission excluded “dial-up Internet access service” because of “the easy ability to switch among competing dial-up Internet access services. Moreover, the underlying dial-up Internet access service is subject to protections under Title II of the Communications Act. The Commission’s interpretation of those protections has resulted in a market for dial-up Internet access that does not present the same concerns as the market for broadband Internet access.” This is a frank acknowledgement that if the Commission had not eliminated Open Access for broadband facilities then the concerns driving today’s debate of “Net Neutrality” would not exist. If the Commission reinstates Open Access then the underlying concerns will go away and regulation of Internet access will not be necessary.

This definition has not been adequately subjected to critical analysis. There are some potential problems and a better definition can be devised.

First, the definition may capture activities beyond merely Internet access. *Open Internet Order* ¶¶ 47 and 52 stressed that it was not supposed to include activities that appeared to meet the definition in whole or in part, such as “virtual private network services, content delivery network services, multichannel video programming services, hosting or data storage services, or Internet backbone services (if those services are separate from broadband Internet access service)” or “coffee shops, bookstores, airlines, and other entities when they acquire Internet service from a broadband provider to enable their patrons to access the Internet from their establishments.” That is fine so far as it goes, but the list is not exhaustive. There are other activities that are not listed and meet the definition. For example, an open proxy server that facilitates requests using all protocols and extending to “substantially all Internet endpoints” would meet the definition.¹¹⁵

Second, the definition does not focus on the transmission component, and that is one of the reasons the definition may be stretched past its intended limitations. The primary differentiating quality of the activity sought to be regulated (broadband Internet access) and other activities that need not be regulated and should not be regulated is the *broadband transmission link* between the provider and end user. Without this link there is no access. Other activities that are not intended to be covered (like the proxy server example above) do not come with transmission. While this point is illustrated by the focus on transmission type in the definitions for fixed and mobile, i2Coalition has recommended that the two types be treated the same, and have the same text. Any justifiable differential treatment based on network technologies used for

¹¹⁵ TOR proxies, for example, support more than just web requests, and provide connectivity to virtually the entire Internet.

the transmission portion should be resolved through the reasonable network management exception. But even if the differential treatment is maintained the main definition should also include transmission as a distinguishing and qualifying characteristic.

A preferable definition can be pulled from § 706. The Commission maintains that § 706 is an important source of authority for the contemplated rules. While i2Coalition does not believe § 706 is sufficient, it is relevant. The alternative definition supplied below draws heavily from § 706, and then adds some of the components in the existing rule.

(a) Broadband Internet Access Service. A mass-market retail service, without regard to any transmission media or technology, that provides high-speed, switched, broadband telecommunications capability and allows the retail user purchasing broadband telecommunications links and any bundled or ancillary functionalities to (1) originate and receive high-quality voice, data, graphics, video and other information content of the user's choosing, (2) obtain applications, services and content from one or more Edge Providers, and/or (3) communicate with other end users or endpoints on the Internet. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence, or that is used to evade the protections set forth in this Part.

3. Definition of “Edge Provider” (8.11(c))

This proposed definition uses other terms of art that are not themselves defined in the proposed rules. i2Coalition believes that definitions for “application” and “content” are also needed. Proposed definitions for these terms are supplied below.

4. Definition of “Fixed broadband Internet access service” (8.11(e))

The terminology used in this rule (and the one for mobile) could lead to disputes over whether a given service is mobile or fixed wireless broadband. If the no-blocking differences are maintained, then given the material regulatory differences under the proposed rules between a fixed wireless service and mobile service, providers will be much incented to call the service mobile but others will want to label it fixed. Since there may be different reasonable network

management outcomes depending on whether a service is mobile or fixed the terms do need to be defined. The final rules must be clear, which the current proposed rules are not.

Assume that a wireless user has a 4G capable router (with or without an externally-mounted antenna) that distributes the signal to desktops, laptops, tablets or smartphones using Wi-Fi. The router can in fact operate while in motion, assuming it is powered from some form of battery. But even if the router is stationary several of the other devices (laptop, tablet, smartphone) that connect to it are not. Does this type of arrangement serve end users primarily at fixed endpoints using stationary equipment? If the router is the endpoint then the answer is yes. If the other devices are the endpoints that matter, then the answer is no.

Second, a mobile station can be “stationary” at certain times, or even most of the time and still be a mobile station. In one case before the Commission, complaining parties claimed that a wireless device and associated service was fixed based on the size and the difficulty associated with moving it about, as well as the fact that it tended to be stationary most of the time. A “laptop-sized wireless access unit” powered from an electrical outlet or by battery that was “approximately 2.76 inches x 12.9 inches x 11.8 inches and weigh[ed] 8.3 pounds including the built-in battery” that came with a short antenna and “a larger high gain antenna for exterior mounting” was found to be a mobile station because it could move, could operate while in motion, and had been operated while in motion in some instances.¹¹⁶

i2Coalition recommends that the final rule delete “using stationary equipment.” There does not appear to be much caselaw on what stationary would mean. The definition for “fixed

¹¹⁶ *In the Matter of Petition of the State Independent Alliance and the Independent Telecommunications Group for a Declaratory Ruling that the Basic Universal Service Offering Provided by Western Wireless in Kansas is Subject to Regulation as Local Exchange Service*, Memorandum Opinion and Order, 17 FCC Rcd 14802 (2002), vacated, dismissed as moot, Order on Reconsideration, 22 FCC Rcd 12015 (2007).

station” at 47 C.F.R. § 1.907 is clearer.¹¹⁷ The Commission has far more experience with applying this definition in specific contexts. Then the Commission should make clear that the station under inquiry is the one that makes the direct connection to the wireless network, and authenticates on that network, rather than other devices that receive information via the station’s router capabilities.

5. Definition of “Mobile broadband Internet access service” (8.11(f))

The reference to “mobile stations” as the qualifier for what is a “Mobile broadband Internet access service” can also lead to disputes over whether a given service that relies on spectrum for transport is mobile or fixed.

The Act and Commission rules have several different definitions and they are not all the same. The Act (§ 153(34)) defines a mobile station as “a radio-communication station capable of being moved and which ordinarily does move.” The definition for “mobile station” in 47 C.F.R. § 1.907 exactly matches the statutory definition. On the other hand, 47 C.F.R. §§ 22.99¹¹⁸ and 27.4¹¹⁹ employ slightly different definitions. The Commission should specify one definition that will apply. i2Coalition recommends that the statutory definition, and therefore also the one at § 1.907, be used. This will not fully flesh out potential disputes, but it will at least eliminate arguments over which definition applies.

6. Additional Definitions

As noted above, i2Coalition believes that certain terms used in the proposed rules but do not have definitions should be defined as part of the final rules. Suggested definitions for those terms are:

¹¹⁷ “Fixed station. A station operating at a fixed location.”

¹¹⁸ “One or more transmitters that are capable of operation while in motion.”

¹¹⁹ “A station in the mobile service intended to be used while in motion or during halts at unspecified points.”

Application. 1. Software that embodies the primary logic characterizing and supporting an end-user service and its features. Such an application may reside on an application server within a service provider's network or may be a 3rd party application outside of a service provider network. 2. Software on user devices providing something of value consumed by the end user. E.g., Microsoft Word, Firefox Web Browser or Google Maps. 3. Software that performs a specific task or function, such as word-processing, creation of spreadsheets, generation of graphics, facilitating electronic mail, etc. Synonym application software.¹²⁰

Content. Any information concerning the substance, purport, or meaning of a communication.

IX. CONCLUSION

The discriminatory practices that the Commission is attempting to address in this proceeding are the direct result of the absence of competition in the broadband market. The proposed rules would regulate Internet access providers' actions, but would not address the root problem. Only Open Access would allow competition and consumer choice back into the broadband access market. i2Coalition recommends that the Commission return to the Open Access policies that first brought us the open Internet by reclassifying the broadband transmission component as a telecommunications service under Title II.

¹²⁰ This proposed definition was taken from the ATIS Telecom Glossary (© Alliance for Telecommunications Industry Solutions), available at <http://www.atis.org/glossary/definition.aspx?id=5445>.